Cisco Secure Firewall ASA Series Command Reference, S Commands

First Published: 2005-05-31

Last Modified: 2023-12-08

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

sa - shov

same-security-traffic

To permit communication between interfaces with equal security levels, or to allow traffic to enter and exit the same interface, use the **same-security-traffic** command in global configuration mode. To disable the same-security traffic, use the **no** form of this command.

same-security-traffic permit { **inter-interface | intra-interface** }
no same-security-traffic permit { **inter-interface | intra-interface** }

Syntax Description

inter-interface	Permits communication between different interfaces that have the same security level.
intra-interface	Permits communication in and out of the same interface.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The **intra-interface** keyword now allows all traffic to enter and exit the same interface, and not just IPsec traffic.

Usage Guidelines

Allowing communication between same security interfaces (enabled by the **same-security-traffic inter-interface** command) provides the following benefits:

- You can configure more than 101 communicating interfaces. If you use different levels for each interface, you can configure only one interface per level (0 to 100).
- You can allow traffic to flow freely between all same security interfaces without access lists.

The **same-security-traffic intra-interface** command lets traffic enter and exit the same interface, which is normally not allowed. This feature might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it might be re-encrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the Secure Firewall ASA is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the ASA and then out again to the other spoke.

Note All traffic allowed by the **same-security-traffic intra-interface** command is still subject to firewall rules. Be careful not to create an asymmetric routing situation that can cause return traffic not to traverse the ASA.

Examples

The following example shows how to enable the same-security interface communication:

```
ciscoasa(config)# same-security-traffic permit inter-interface
```

The following example shows how to enable traffic to enter and exit the same interface:

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

Related Commands

Command	Description
show running-config same-security-traffic	Displays the **same-security-traffic** configuration.

sasl-mechanism

To specify a SASL (Simple Authentication and Security Layer) mechanism for authenticating an LDAP client to an LDAP server, use the **sasl-mechanism** command in aaa-server host configuration mode. The SASL authentication mechanism options are **digest-md5** and **kerberos** .

To disable an authentication mechanism, use the **no** form of this command.

sasl-mechanism { **digest-md5 | kerberos server-group-name** }
no sasl-mechanism { **digest-md5 | kerberos server-group-name** }

Note Because the ASA serves as a client proxy to the LDAP server for VPN users, the LDAP client referred to here is the ASA.

Syntax Description

digest-md5	The ASA responds with an MD5 value computed from the username and password.
kerberos	The ASA responds by sending the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism.
server-group-name	Specifies the Kerberos aaa-server group, up to 64 characters.

Command Default

No default behavior or values. The ASA passes the authentication parameters to the LDAP server in plain text.

Note We recommend that you secure LDAP communications with SSL using the **ldap-over-ssl** command if you have not configured SASL.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Use this command to specify ASA authentication to an LDAP server using SASL mechanisms.

Both the ASA and the LDAP server can support multiple SASL authentication mechanisms. When negotiating SASL authentication, the ASA retrieves the list of SASL mechanisms configured on the server and sets the authentication mechanism to the strongest mechanism configured on both the ASA and the server. The Kerberos mechanism is stronger than the Digest-MD5 mechanism. To illustrate, if both the LDAP server and the ASA support both mechanisms, the ASA selects Kerberos, the stronger of the mechanisms.

When disabling the SASL mechanisms, you must enter a separate **no** command for each mechanism you want to disable because they are configured independently. Mechanisms that you do not specifically disable remain in effect. For example, you must enter both of the following commands to disable both SASL mechanisms:

no sasl-mechanism digest-md5
no sasl-mechanism kerberos server-group-name

Examples

The following examples, entered in aaa-server host configuration mode, enable the SASL mechanisms for authentication to an LDAP server named ldapsvr1 with an IP address of 10.10.0.1. This example enables the SASL digest-md5 authentication mechanism:

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism digest-md5
```

The following example enables the SASL Kerberos authentication mechanism and specifies kerb-servr1 as the Kerberos AAA server:

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

saml idp

To add a new SAML IdP, use the saml idp command in webvpn configuration mode. To remove a SAML IdP, use the no form of this command.

saml idp *idp-entityID*
no saml idp *idp-entityID*

Syntax Description

base-URL	The Clientless VPN's base URL. It is used in SAML metadata that is provided to third-party IdPs, so that IdPs can redirect end users back to the ASA.
clock-skew <*value*>	Clock skew which will tolerate the NotBefore and NotOnOrAfter SAML assertions. By default the clock-skew should be disabled. The default value for the clock-skew is 1 second. The allowed range is 1 - 180 seconds.
idp-entityID	The entity ID of the SAML Idp you are configuring the ASA to use.
internal	Set this flag if the IdP is in the internal network.
signature signature <value>	Enable or disable signature in a SAML request. (Optional) Enable signature and use a specific method in a SAML request.
timeout assertion	Overrides NoOnOrAfter if the sum of NotBefore and timeout is earlier than NoOnOrAfter.
timeout-in-seconds	The SAML timeout value in seconds. By default, there is no SAML timeout. NotBefore and NotOnOrAfter in the assertion is used to determine the validity.
trustpoint [idp | sp] <*trustpoint-name*>	The trustpoint idp contains the IdP certificate for ASA to verify SAML assertions. The trustpoint-name is one of the existing trustpoint names. The trustpoint sp contains the ASA (SP's) certificate for IdP to verify the ASA's signature or encrypt SAML assertion.
url [sign-in | sign-out] <*value*>	The URL is the IdP's sign-in and sign-out URL. The value of the URL for signing into the IdP. The url value must contain 4 to 2000 characters.

Command Default

None.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.
9.7(1)	The internal attribute was added.
9.8(1)	Added SHA2 support and the ability to specify a signature method in a SAML request.

Usage Guidelines

This command configures one or more third party SAML identity provider's settings. The IdP settings are not used until they are applied in a tunnel group.

The SAML IdP's sign-in url, sign-out url, signing certificate can be found on the vendor's website. You must create a trustpoint to hold the IdP's signing certificate. The trustpoint name will be used by trustpoint idp.

Creating an Idp in webvpn mode puts you into saml-idp sub-mode, where you configure the following settings for this Idp:

- url sign-in—URL to sign in to the Idp.
- url sign-out—URL for redirecting to when signing out of the IdP.
- signature—Enable or disable signature in SAML request. By default, the signature is disabled.
- signature <value>—Enable signature and specify the method as rsa-sha1, rsa-sha256, rsa-sha384, or rsa-sha512. By default the signature is disabled.
- time-out—SAML timeout value in seconds.
- base-url—URL is provided to third-party IdPs to redirect end-users back to the ASA. When base-url is not configured, the URL comes from the ASA’s hostname and domain-name. For example, https://ssl-vpn.cisco.com as the base URL in show saml metadata when hostname is “ssl-vpn” and domain name is “cisco.com.” If neither base-url or hostname/domain-name are configured, show saml metadata returns an error.
- trustpoint—Assigns an existing trustpoint based on the ASA (SP)'s or IDP certificate that the IdP can use to verify ASA's signature or encrypt SAML assertion.

Examples

The following example shows how to define an Idp, and configure the Idp settings:

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config-webvpn)# saml idp salesforce_idp

ciscoasa(config-webvpn-saml-idp)# url sign-in
 https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect

ciscoasa(config-webvpn-saml-idp)# url sign-out
 https://asa-dev-ed.my.salesforce.com/idp/endpoint/HttpRedirect
ciscoasa(config-webvpn-saml-idp)# trustpoint idp salesforce_trustpoint
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_trustpoint
ciscoasa(config-webvpn)# saml idp feide_idp

ciscoasa(config-webvpn-saml-idp)# url sign-in
http://cisco.feide.no/simplesaml/saml2/idp/SSOService.php

ciscoasa(config-webvpn-saml-idp)# trustpoint idp feide_trustpoint
ciscoasa(config-webvpn-saml-idp)# trustpoint sp asa_trustpoint
ciscoasa(config-webvpn-saml-idp)# signature
ciscoasa(config-webvpn-saml-idp)# timeout assertion 120
ciscoasa(config-webvpn-saml-idp)# base-url https://ssl-vpn.cisco.com
```

Related Commands

Command	Description
authentication	Sets the authentication type for a tunnel group, such as saml.
identity-provider	Names this configuration of a third-party SAML identity provider in the ASA.

saml idp-trustpoint

To override the trustpoint IdP setting in the SAML IdP configuration, use the **saml idp-trustpoint** command in the webvpn tunnel group configuration mode. To remove the IdP trustpoint settings, use the no form of the command

saml idp-trustpoint *name*
no saml idp-trustpoint *name*

Syntax Description

name	Name of the IdP trustpoint.

Command Default

Not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
config-tunnel-webvpn	• Yes	• Yes	• Yes	• No	—

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

Existing ASA SAML configurations support only one IDP trustpoint for each configured SAML IDP. The **saml idp-trustpoint** command overrides the IdP settings to support the Microsoft Azure multiple application deployment scenario.

If the IdP trustpoint setting is present in the tunnel-group, the command overrides the trustpoint IdP setting in the IdP configuration, which is referenced by the **saml identity-provider** command in the tunnel group.

Examples

The following example shows how to override the IdP settings in trustpoint IdP configuration:

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config-webvpn)# tunnel-group Sales webvpn-attributes
ciscoasa(config-tunnel-webvpn)# saml idp-trustpoint _SmartCallHome_ServerCA
```

Related Commands

Command	Description
identity-provider	Names configuration of a third-party SAML identity provider in the ASA.

saml identity-provider

Use this CLI in config-tunnel-webvpn mode to assign a SAML IdP to a tunnel group (connection profile)

saml identity-provider *name*
no saml identity-provider *name*

Syntax Description

name	The name of the SAML Idp you are configuring the ASA to use.

Command Default

None.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This names this configuration of a third-party SAML identity provider in the ASA.

Note While adding the SAML identity provider name, if you get the error "ERROR: SAML configuration could not be built", check your tunnel group name to ensure that the tunnel-group name does not contain the following special characters: &, ", or <. The tunnel group name is added using the **tunnel-group webvpn-attributes** command.

Related Commands

Command	Description
authentication	Sets the authentication type for a tunnel group, such as saml.
idp	Sets the Idp for a third-party SAML identity provider.

sast

To specify the number of SAST certificates to create in the CTL record, use the **sast** command in ctl-file configuration mode. To set the number of SAST certificates in the CTL file back to the default value of 2, use the **no** form of this command.

sast *number_sasts*
no sast *number_sasts*

Syntax Description

number_sasts	Specifies the number of SAST keys to create. The default is 2. The maximum allowed is 5.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl-file configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	The command was added.

Usage Guidelines

CTL files are signed by a System Administrator Security Token (SAST).

Because the Phone Proxy generates the CTL file, it needs to create the SAST key to sign the CTL file itself. This key can be generated on the ASA. A SAST is created as a self-signed certificate.

Typically, a CTL file contains more than one SAST. In case a SAST is not recoverable, the other one can be used to sign the file later.

Examples

The following example shows the use of the **sast** command to create 5 SAST certificates in the CTL file:

```
ciscoasa
(
config-ctl-file
)# sast 5
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.

Command	Description
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

scansafe

To enable Cloud Web Security inspection for a context, use the **scansafe** command in context configuration mode. To disable Cloud Web Security, use the **no** form of this command.

scansafe [**license** *key*]
no scansafe [**license** *key*]

Syntax Description

license *key*	Enters an authentication key for this context. If you do not specify a key, the context uses the license configured in the system configuration. The ASA sends the authentication key to the Cloud Web Security proxy servers to indicate from which organization the request comes. The authentication key is a 16-byte hexadecimal number.

Command Default

By default, the context uses the license entered in the system configuration.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

In multiple context mode, you must allow Cloud Web Security per context.

Examples

The following sample configuration enables Cloud Web Security in context one with the default license and in context two with the license key override:

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http [**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server { **primary** | **backup** }	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it’s the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

scansafe general-options

To configure communication with the Cloud Web Security proxy server, use the **scansafe general-options** command in global configuration mode. To remove the server configuration, use the **no** form of this command.

scansafe general-options
no scansafe general-options

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You can configure a primary and backup proxy server for Cloud Web Security.

Examples

The following example configures a primary server:

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
health-check application	Enables Cloud Web Security application health checking for failover.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.

Command	Description
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it’s the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

scep-enrollment enable

To enable or disable the Simple Certificate Enrollment Protocol for a tunnel group, use the **scep-enrollment enable** command in tunnel-group general-attributes mode.

To remove the command from the configuration, use the **no** form of this command.

scep-enrollment enable
no scep-enrollment enable

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is not present in the tunnel group configuration.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

Only the Cisco Secure Client, Release 3.0 and later, supports this feature.

The ASA can proxy SCEP requests between Secure Client and a third-party certificate authority. The certificate authority only needs to be accessible to the ASA if it is acting as the proxy. For the ASA to provide this service, the user must authenticate using any of the methods supported by AAA before the ASA sends an enrollment request. You can also use Host Scan and dynamic access policies to enforce rules of eligibility to enroll.

The ASA supports this feature only with an AnyConnect SSL or IKEv2 VPN session. It supports all SCEP-compliant certificate authorities, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA.

Clientless (browser-based) access does not support SCEP Proxy, although WebLaunch—clientless-initiated Secure Client—does support it.

The ASA does not support polling for certificates.

The ASA supports load balancing for this feature.

Examples

The following example, entered in global configuration mode, creates a remote access tunnel group named remotegrp and enables SCEP for the group policy:

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this option.
```

Related Commands

Command	Description
crypto ikev2 enable	Enables IKEv2 negotiation on the interface on which IPsec peers communicate.
scep-forwarding-url	Enrolls the SCEP certificate authority for the group policy.
secondary-pre-fill-username clientless	Supplies a common, secondary password when a certificate is unavailable for WebLaunch support of the SCEP proxy.
secondary-authentication-server-group	Supplies the username when a certificate is unavailable.

scep-forwarding-url

To enroll an SCEP certificate authority for a group policy, use the **scep-forwarding-url** command in group-policy configuration mode.

To remove the command from the configuration, use the **no** form of this command.

scep-forwarding-url { **none | value** [*URL*] }
no scep-forwarding-url

Syntax Description

none	Specifies no certificate authority for the group policy.
URL	Specifies the SCEP URL of the certificate authority.
value	Enables this feature for clientless connections.

Command Default

By default, this command is not present.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

Enter this command once per group policy to support a third-party digital certificate.

Examples

The following example, entered in global configuration mode, creates a group policy named FirstGroup and enrolls a certificate authority for the group policy:

```
ciscoasa(config)# group-policy FirstGroup internal
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
Attempting to retrieve the CA/RA certificate(s) using the URL. Please wait ...
```

Related Commands

Command	Description
crypto ikev2 enable	Enables IKEv2 negotiation on the interface on which IPsec peers communicate.
scep-enrollment enable	Enables Simple Certificate Enrollment Protocol for a tunnel group.

Command	Description
secondary-pre-fill-username clientless	Supplies a common, secondary password when a certificate is unavailable for WebLaunch support of the SCEP proxy.
secondary-authentication-server-group	Supplies the username when a certificate is unavailable.

secondary

To set the preferred unit for a failover group when using the **preempt** command, use the **secondary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

secondary
no secondary

Syntax Description

This command has no arguments or keywords.

Command Default

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Failover group configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Earlier software versions allowed “simultaneous” boot up so that the failover groups did not require the **preempt** command to become active on the preferred unit. However, this functionality has now changed so that both failover groups become active on the first unit to boot up.

Usage Guidelines

Assigning a **primary** or **secondary** preference to a failover group specifies which unit the failover group becomes active on when you set the **preempt** command. Both failover groups become active on the first unit that boots up (even if it seems like they boot simultaneously, one unit becomes active first), despite the **primary** or **secondary** setting for the group. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
primary	Gives the primary unit a higher priority than the secondary unit.

secondary-authentication-server-group

To specify a secondary authentication server group to associate with the session when double authentication is enabled, use the **secondary-authentication-server-group** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

secondary-authentication-server-group [*interface_name*] { **none | LOCAL |** *groupname* [**LOCAL**] } [**use-primary-username**]
no secondary-authentication-server-group

Syntax Description

interface_name	(Optional) Specifies the interface where the IPsec tunnel terminates.
LOCAL	(Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either **LOCAL** or **NONE,** do not use the **LOCAL** keyword here.
none	(Optional) Specifies the server group name as **NONE** , indicating that authentication is not required.
groupname [**LOCAL**]	Identifies the previously configured authentication server or group of servers. Optionally, this can be the LOCAL group.
use-primary-username	Use the primary username as the username for the secondary authentication.

Command Default

The default value is **none** .

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **secondary-authentication-server-group** command specifies the secondary AAA server group. The secondary server group cannot be an SDI server group.

If the use-primary-username keyword is configured, then only one username is requested in the login dialog.

If the usernames are extracted from a digital certificate, only the primary username is used for authentication.

Examples

The following example, entered in global configuration mode, creates a remote access tunnel group named remotegrp and specifies the use of the group sdi_server as the primary server group and the group ldap_ server as the secondary authentication server group for the connection:

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-webvpn)# authentication-server-group sdi_server
ciscoasa(config-tunnel-webvpn)# secondary-authentication-server-group ldap_server
ciscoasa(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

secondary-color

To set a secondary color for the WebVPN login, home page, and file access page, use the **secondary-color** command in webvpn configuration mode. To remove a color from the configuration and reset the default, use the **no** form of this command.

secondary-color [*color*]
no secondary-color

Syntax Description

color (Optional) Specifies the color. You can use a comma separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.
- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.
- Name length maximum is 32 characters

Command Default

The default secondary color is HTML #CCCCFF, a lavender shade.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The number of RGB values recommended for use is 216, many fewer than the mathematical possibilities. Many displays can handle only 256 colors, and 40 of those look differently on MACs and PCs. For best results, check published RGB tables. To find RGB tables online, enter RGB in a search engine.

Examples

The following example shows how to set an HTML color value of #5F9EAO, which is a teal shade:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# secondary-color #5F9EAO
```

Related Commands

Command	Description
title-color	Sets a color for the WebVPN title bar on the login, home page, and file access page

secondary-pre-fill-username

To enable the extraction of a username from a client certificate for use in double authentication for a clientless or an Secure Client connection, use the **secondary-pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

secondary-pre-fill-username { **clientless** | **ssl-client** } [**hide**]
secondary-pre-fill-username { **clientless** | **ssl-client** } **hide** [**use-primary-password** | **use-common-password** [*type_num*] *password*]
no secondary-pre-fill-username

Syntax Description

clientless	Enables this feature for clientless connections.
hide	Hides the username to be used for authentication from the VPN user.
password	Enter the password string.
client **ssl-client**	Enables this feature for AnyConnect VPN client connections. Use the **client** keyword in 9.8(1)+.
type_num	Enter one of the following options: • 0 if the password to be entered is plain text. • 8 if the password to be entered is encrypted. The password appears as asterisks as you type.
use-common-password	Specifies a common secondary authentication password to use without prompting the user for it.
use-primary-password	Reuses the primary authentication password for secondary authentication without prompting the user for it.

Command Default

This feature is disabled by default. Entering this command without the **hide** keyword reveals the extracted username to the VPN user. The user receives a password prompt if you specify neither the use-primary-password nor the use-common-password keywords. The default value of *type_num* is 8.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
8.3(2)	The [**use-primary-password** | **use-common-password** [*type_num*] *password*] option was added.
9.8(1)	The **ssl-client** keyword was changed to **client**.

Usage Guidelines

To enable this feature, you must also enter the **secondary-username-from-certificate** command in tunnel-group general-attributes mode.

This command is meaningful only if double authentication is enabled. The **secondary-pre-fill-username** command enables the use of a username extracted from the certificate field specified in the **secondary-username-from-certificate** command as the username for secondary username/password authentication. To use this secondary-pre-fill username-from-certificate feature, you must configure both commands.

Note Clientless and SSL-client connections are not mutually exclusive options. Only one can be specified per command line, but both can be enabled at the same time.

If you hide the second username and use a primary or common password, the user experience is similar to single authentication. Using the primary or common password makes the use of device certificates to authenticate a device a seamless user experience.

The **use-primary-password** keyword specifies the use of the primary password as the secondary password for all authentications.

The **use-common-password** keyword specifies the use of a common secondary password for all secondary authentications. If a device certificate installed on the endpoint contains a BIOS ID or some other identifier, a secondary authentication request can use the pre-filled BIOS ID as the second username and use a common password configured for all authentications in that tunnel group.

Examples

The following example creates an IPsec remote access tunnel group named remotegrp, and specifies the reuse of a name from the digital certificate on the endpoint as the name to be used for an authentication or authorization query when the connections are browser-based.

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless
```

The following example performs the same function as the previous command, but hides the extracted username from the user:

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
```

The following example performs the same function as the previous command, except that it applies only to Secure Client connections:

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client hide
```

The following example hides the username and reuses the primary authentication password for secondary authentication without prompting the user:

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client hide use-primary-password
```

The following example hides the username and uses the password you enter for secondary authentication:

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client hide use-common-password
 **********
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

secondary-text-color

To set the secondary text color for the WebVPN login, home page and file access page, use the **secondary-text-color** command in webvpn mode. To remove the color from the configuration and reset the default, use the **no** form of this command.

secondary-text-color [*black* | *white*]
no secondary-text-color

Syntax Description

auto	Chooses black or white based on the settings for the text-color command. That is, if the primary color is black, this value is white.
black	The default secondary text color is black.
white	You can change the text color to white.

Command Default

The default secondary text color is black.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example shows how to set the secondary text color to white:

```
ciscoasa
(config)#
 webvpn
ciscoasa(config-webvpn)# secondary-text-color white
```

Related Commands

Command	Description
text-color	Sets a color for text in the WebVPN title bar on the login, home page and file access page

secondary-username -from-certificate

To specify the field in a certificate to use as the secondary username for double authentication for a clientless or AnyConnect (SSL-client) connection, use the **secondary-username-from-certificate** command in tunnel-group general-attributes mode.

To remove the attribute from the configuration and restore default values, use the **no** form of this command.

secondary-username-from-certificate { *primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script** }
no secondary-username-from-certificate

Syntax Description

primary-attr	Specifies the attribute to use to derive a username for an authorization query from a certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a username for an authentication or authorization query from a digital certificate. If pre-fill-username is enable, the derived name can also be used in an authentication query.
use-entire-name	Specifies that the ASA must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.
use-script	Specifies the use of a script file generated by Adaptive Security Device Manager (ASDM) to extract the DN fields from a certificate for use as a username.

Command Default

This feature is disabled by default and is meaningful only when double authentication is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general-attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command is meaningful only when double authentication is enabled.

When double authentication is enabled. this command selects one or more fields in a certificate to use as the username. The **secondary-username-from-certificate** command forces the security appliance to use the specified certificate field as the second username for the second username/password authentication.

To use this derived username in the pre-fill username from certificate feature for the secondary username/password authentication or authorization, you must also configure the **pre-fill-username** and **secondary-pre-fill-username** commands in tunnel-group webvpn-attributes mode. That is, to use the secondary pre-fill username feature, you must configure both commands.

Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.
use-entire-name	Use entire DN name. Not available a s a secondary attribute.
use-script	Use a script file generated by ASDM.

Note If you also specify the **secondary-authentication-server-group** command, along with the **secondary-username-from-certificate command, only** the primary username is used for authentication.

Examples

The following example, entered in global configuration mode, creates a remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute and OU as the secondary attribute to use to derive a name for an authorization query from a digital certificate:

```
ciscoasa(config)# tunnel-group remotegrp type remote-access
ciscoasa(config)# tunnel-group remotegrp general-attributes
ciscoasa(config-tunnel-general)# username-from-certificate CN
ciscoasa(config-tunnel-general)# secondary-username-from-certificate OU
ciscoasa(config-tunnel-general)#
```

The following example shows how to modify the tunnel-group attributes to configure the pre-fill username.

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
 secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
secondary-pre-fill-username	Enables username extraction for clientless or Secure Client connection
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
secondary-authentication-server-group	Specifies the secondary AAA server group. If the usernames are extracted from a digital certificate, only the primary username is used for authentication.

secondary-username-from-certificate-choice

To select the certificate from where the username should be used for pre-fill username field for secondary authentication or authorization, use the **secondary-username-from-certificate-choice** command. Use this command in tunnel-group general-attributes mode. To use the username from the default certificate, use the **no** form of the command.

secondary-username-from-certificate-choice { **first-certificate | second-certificate** }
no secondary-username-from-certificate-choice { **first-certificate | second-certificate** }

Syntax Description

first-certificate	Specifies if the username from the machine certificate sent in SSL or IKE to be used in pre-fill username field for secondary authentication.
second-certificate	Specifies if the username from the user certificate from client to be used in pre-fill username field for secondary authentication.

Command Default

The username for prefill is retrieved from the second certificate by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.14(1)	This command was added.

Usage Guidelines

The multiple certificates option allows certificate authentication of both the machine and user via certificates. The pre-fill username field allows a field from the certificates to be parsed and used for subsequent (primary and secondary)AAA authentication in a AAA and certificate authenticated connection. The username for prefill is always retrieved from the second (user) certificate received from the client.

Beginning with 9.14(1), ASA allows you to choose whether the first certificate (machine certificate) or second certificate (user certificate) should be used to derive the username for the pre-fill username field.

This command is available and can be configured for any tunnel groups irrespective of the authentication type (aaa, certificate, or multiple-certificate). However, the configuration takes effect only for Multiple Certificate Authentication (multiple-certificate or aaa multiple-certificate). When the option is not used for Multiple Certificate Authentication, the second certificate is used by default for authentication or authorization purpose.

Examples

The following example shows how to configure the certificate to be used for prefill username for primary and secondary authentication or authorization:

```
ciscoasa(config)#tunnel-group tg1 type remote-access
ciscoasa(config)#tunnel-group tg1 general-attributes
ciscoasa(config-tunnel-general)# address-pool IPv4
ciscoasa(config-tunnel-general)# secondary-authentication-server-group LOCAL/<Auth-Server>

ciscoasa(config-tunnel-general)# username-from-certificate-choice first-certificate
ciscoasa(config-tunnel-general)# secondary-username-from-certificate-choice first-certificate
ciscoasa(config)# tunnel-group tg1 webvpn-attributes
ciscoasa(config-tunnel-webvpn)# authentication aaa multiple-certificate
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username client
```

Related Commands

Command	Description
username-from-certificate-choice	Specify the certificate option for primary authentication.

secure-unit-authentication

To enable secure unit authentication, use the **secure-unit-authentication enable** command in group-policy configuration mode. To disable secure unit authentication, use the **secure-unit-authentication disable** command. To remove the secure unit authentication attribute from the running configuration, use the **no** form of this command.

secure-unit-authentication { **enable | disable** }
no secure-unit-authentication

Syntax Description

disable	Disables secure unit authentication.
enable	Enables secure unit authentication.

Command Default

Secure unit authentication is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Secure unit authentication requires that you have an authentication server group configured for the tunnel group the hardware client(s) use.

If you require secure unit authentication on the primary ASA, be sure to configure it on any backup servers as well.

The **no** option allows inheritance of a value for secure unit authentication from another group policy.

Secure unit authentication provides additional security by requiring VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel. With this feature enabled, the hardware client does not have a saved username and password.

Note With this feature enabled, to bring up a VPN tunnel, a user must be present to enter the username and password.

Examples

The following example shows how to enable secure unit authentication for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# secure-unit-authentication
 enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN hardware client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
user-authentication	Requires users behind a hardware client to identify themselves to the ASA before connecting.

security-group

To add a security group to a security object group for use with Cisco TrustSec, use the **security-group** command in object-group security configuration mode. To remove the security group, use the **no** form of this command.

security-group { **tag** *sgt##* | **name** *sg_name* }
no security-group { **tag** *sgt##* | **name** *sg_name* }

Syntax Description

tag *sgt#*	Specifies the security group object as an inline tag. Enter a number from 1 to 65533 for a Tag security type. An SGT is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB) by the ISE. Security group names are created on the ISE and provide user-friendly names for security groups. The security group table maps SGTs to security group names.
name *sg_name*	Specifies the security group object as a named object. Enter a 32-byte case-sensitive string for a Name security type. The *sg_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.].

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object-group security configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

You can create security group object groups for use in features that support Cisco TrustSec by including the group in an extended ACL, which in turn can be used in an access rule, for example.

When integrated with Cisco TrustSec, the ASA downloads security group information from the ISE. The ISE acts as an identity repository, by providing Cisco TrustSec tag to user identity mapping and Cisco TrustSec tag to server resource mapping. You provision and manage security group access lists centrally on the ISE.

However, the ASA might have localized network resources that are not defined globally that require local security groups with localized security policies. Local security groups can contain nested security groups that are downloaded from the ISE. The ASA consolidates local and central security groups.

To create local security groups on the ASA, you create a local security object group. A local security object group can contain one or more nested security object groups or Security IDs or security group names. User can also create a new Security ID or security group name that does not exist on the ASA.

You can use the security object groups you create on the ASA to control access to network resources. You can use the security object group as part of an access group or service policy.

Examples

The following example shows how to configure a security group object:

```
ciscoasa(config)# object-group security mktg-sg
ciscoasa(config)# security-group name mktg
ciscoasa(config)# security-group tag 1
```

The following example shows how to configure a security group object:

```
ciscoasa(config)# object-group security mktg-sg-all
ciscoasa(config)# security-group name mktg-managers
ciscoasa(config)# group-object mktg-sg // nested object-group
```

Related Commands

Command	Description
object-group security	Creates a security group object.

security-group-tag

To configure a security group tag attribute in a remote access VPN group policy or for a user in the LOCAL user database, use the **security-group-tag value** command in group-policy or username configuration mode. To remove the security group tag attribute, use the **no** form of this command.

security-group-tag { **none | value** *sgt* }
no security-group-tag { **none | value** *sgt* }

Syntax Description

none	Do not set a security group tag for this group policy or user.
value *sgt*	Specifies the security group tag number.

Command Default

The default is **security-group-tag none**, which means that there is no security group tag in this attribute set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy or username configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

ASA supports security group tagging of VPN sessions. You can assign a Security Group Tag (SGT) to a VPN session using an external AAA server, or by configuring a security group tag for a local user or for a VPN group policy. This tag can then be propagated through the Cisco TrustSec system over Layer 2 Ethernet. Security group tags are useful on group policies and for local users when the AAA server cannot provide an SGT.

Following is the typical process for assigning an SGT to a VPN user:

1. A user connects to a remote access VPN that uses a AAA server group containing ISE servers.

2. The ASA requests AAA information from ISE, which might include an SGT. The ASA also assigns an IP address for the user's tunneled traffic.

3. The ASA uses AAA information to authenticate the user and creates a tunnel.

4. The ASA uses the SGT from AAA information and the assigned IP address to add an SGT in the Layer 2 header.

5. Packets that include the SGT are passed to the next peer device in the Cisco TrustSec network.

If there is no SGT in the attributes from the AAA server to assign to a VPN user, then the ASA uses the SGT in the group policy. If there is no SGT in the group policy, then tag 0x0 is assigned.

Examples

The following example shows how to configure SGT attributes for a group policy.

```
ciscoasa(config-group-policy)# security-group-tag value 101
```

Related Commands

Command	Description
show asp table cts sgt-map	Displays the IP address-security group table mapping entries from the IP address-security group table mapping database maintained in the datapath.
show cts sgt-map	Displays the IP address-security group table manager entries in the control path.

security-level

To set the security level of an interface, use the **security-level** command in interface configuration mode. To set the security level to the default, use the **no** form of this command. The security level protects higher security networks from lower security networks by imposing additional protection between the two.

security-level *number*
no security-level

Syntax Description

number	An integer between 0 (lowest) and 100 (highest).

Command Default

By default, the security level is 0.

If you name an interface "inside" and you do not set the security level explicitly, then the ASA sets the security level to 100 (see the **nameif** command). You can change this level if desired.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **nameif** command to an interface configuration mode command.

Usage Guidelines

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines —Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
- NetBIOS inspection engine—Applied only for outbound connections.
- OraServ inspection engine—If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the ASA.
- Filt ering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For same security interfaces, you can filter traffic in either direction.

- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** com mand—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For same security interfaces, you can configure **established** commands for both directions.

Normally, interfaces on the same security level cannot communicate. If you want interfaces on the same security level to communicate, see the **same-security-traffic** command. You might want to assign two interfaces to the same level and allow them to communicate if you want to create more than 101 communicating interfaces, or you want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Examples

The following example configures the security levels for two interfaces to be 100 and 0:

```
ciscoasa(config)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
clear local-host	Resets all connections.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
vlan	Assigns a VLAN ID to a subinterface.

segment-id

To specify the VXLAN ID for a VNI interface, use the **segment-id** command in interface configuration mode. To remove the ID, use the **no** form of this command.

segment-id*id*
no segment-id *id*

Syntax Description

id	Sets the ID between 1 and 16777215.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

The segment ID is used for VXLAN tagging.

Examples

The following example configures the VNI 1 interface and specifies a segment ID of 1000:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.

Command	Description
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

send response

To send a RADIUS Accounting-Response Start and Accounting-Response Stop message to the sender of the RADIUS Accounting-Request Start and Stop messages, use the **send response** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

This option is disabled by default.

send response
no send response

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Radius-accounting parameter configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to send a response with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# send response
ciscoasa(config-pmap-p)# send response
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

seq-past-window

To set the action for packets that have past-window sequence numbers (the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window), use the **seq-past-window** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

seq-past-window { **allow** | **drop** }
no seq-past-window

Syntax Description

allow	Allows packets that have past-window sequence numbers. This action is only allowed if the **queue-limit** command is set to 0 (disabled).
drop	Drops packets that have past-window sequence numbers.

Command Default

The default action is to drop packets that have past-window sequence numbers.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1.**tcp-map**—Identifies the TCP normalization actions.

a.**seq-past-window**—In tcp-map configuration mode, you can enter the **seq-past-window** command and many others.

2.**class-map**—Identify the traffic on which you want to perform TCP normalization.

3.**policy-map**—Identify the actions associated with each class map.

a.**class**—Identify the class map on which you want to perform actions.

b.**set connection advanced-options**—Identify the tcp-map you created.

4.**service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example sets the ASA to allow packets that have past-window sequence numbers:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# seq-past-window allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
queue-limit	Sets the out-of-order packet limit.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

serial-number

To include the ASA serial number in the certificate during enrollment, use the **serial-number** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

serial-number
no serial-number

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to not include the serial number.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the ASA serial number in the enrollment request for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

server (pop3s, imap4s, smtps) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify a default e-mail proxy server, use the **server** command in the applicable e-mail proxy configuration mode. To remove the attribute from the configuration, use the **no** version of this command. The ASA sends requests to the default e-mail server when the user connects to the e-mail proxy without specifying a server. If you do not configure a default server, and a user does not specify a server, the ASA returns an error.

server { *ipaddr or hostname* }
no server

Syntax Description

hostname	The DNS name of the default e-mail proxy server.
ipaddr	The IP address of the default e-mail proxy server.

Command Default

There is no default e-mail proxy server by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s configuration	• Yes	• Yes	—	—	• Yes
Imap4s configuration	• Yes	• Yes	—	—	• Yes
Smtps configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5.2	This command was deprecated.

Examples

The following example shows how to set a default POP3S e-mail server with an IP address. of 10.1.1.7:

```
ciscoasa
(config)#
 pop3s
```

```
ciscoasa(config-pop3s)# server 10.1.1.7
```

server (scansafe general-options)

To configure the primary and backup Cloud Web Security proxy servers, use the **server** command in scansafe general-options configuration mode. To remove the server, use the **no** form of this command.

server { **primary | backup** } { **ip** *ip_address* | **fqdn** *fqdn* } [**port** *port*]
no server { **primary | backup** } { **ip** *ip_address* | **fqdn** *fqdn* } [**port** *port*

Syntax Description

backup	Specifies that you are identifying the backup server.
ip *ip_address*	Specifies the server IP address.
fqdn *fqdn*	Specifies the server fully-qualified domain name (FQDN).
port *port*	(Optional) By default, the Cloud Web Security proxy server uses port 8080 for both HTTP and HTTPS traffic; do not change this value unless directed to do so.
primary	Specifies that you are identifying the primary server.

Command Default

The default port is 8080.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Scansafe general-options configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server. These servers are routinely polled to check for their availability. If your ASA is unable to reach the Cloud Web Security proxy server (for example, if no SYN/ACK packets arrive from the proxy server), then the proxy server is polled through a TCP three-way handshake to check its availability. If the proxy server is unavailable after a configured number of retries (the default is five), the server is declared as unreachable, and the backup proxy server becomes active.

Note You can further refine failover by checking the health of the Cloud Web Security application. In some cases, the server can complete the TCP three-way handshake, yet the Cloud Web Security application on the server is not functioning correctly. If you enable application health checking, the system can fail over to the backup server even if the three-way handshake completes, if the application itself does not respond. This provides a more reliable failover setup. Use the **health-check application** command to enable this extra check.

The ASA automatically falls back to the primary Cloud Web Security proxy server from the backup server after continued polling shows that the primary server is active for two consecutive retry count periods. You can change this polling interval using the **retry-count** command.

Traffic Conditions Under Which Proxy Server Is Not Reachable	Server Timeout Calculation	Connection Timeout Result
High traffic	Client half open connection timeout + ASA TCP connection timeout	(30 + 30) = 60 seconds
Single connection failure	Client half open connection timeout + ((retry threshold - 1) x (ASA TCP connection timeout))	(30 + ((5-1) x (30)) = 150 seconds
Idle—No connections are passing	15 minutes + ((retry threshold) x (ASA TCP connection timeout))	900 + (5 x (30) = 1050 seconds

Examples

The following example configures a primary and backup server. You must enter the command separately for the primary and backup server.

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
health-check application	Enables Cloud Web Security application health checking for failover.
http [**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.

Command	Description
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server { **primary** | **backup** }	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it’s the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current HTTP(S) connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

server (ssh pubkey-chain)

To manually add or delete SSH servers and their keys from the ASA database for the on-board Secure Copy (SCP) client, use the **server** command in ssh pubkey-chain configuration mode. To remove a server and its host key, use the **no** form of this command.

server *ip_address*
no server *ip_address*

Syntax Description

ip_address	Specifies the SSH server IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ssh pubkey-chain configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.1(5)	This command was added.

Usage Guidelines

You can copy files to and from the ASA using the on-board SCP client. The ASA stores the SSH host key for each SCP server to which it connects. You can manually add or delete servers and their keys from the ASA database if desired.

For each server, you can specify the **key-string** (public key) or **key-hash** (hashed value) of the SSH host.

Examples

The following example adds an already hashed host key for the server at 10.86.94.170:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

The following example adds a host string key for the server at 10.7.8.9:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
```

```
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

Related Commands

Command	Description
copy	Copies a file to or from the ASA.
key-hash	Enters a hashed SSH host key.
key-string	Enters a public SSH host key.
ssh pubkey-chain	Manually adds or deletes servers and their keys from the ASA database.
ssh stricthostkeycheck	Enables SSH host key checking for the on-board Secure Copy (SCP) client.

server authenticate-client

To enable the ASA to authenticate the TLS client during TLS handshake, use the **server authenticate-client** command in tls-proxy configuration mode.

To bypass client authentication, use the **no** form of this command.

server authenticate-client
no server authenticate-client

Syntax Description

This command has arguments or keywords.

Command Default

This command is enabled by default, which means the TLS client is required to present a certificate during handshake with the ASA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tls-proxy configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

Use the **server authenticate-client** command to control whether a client authentication is required during TLS Proxy handshake. When enabled (by default), the security appliance sends a Certificate Request TLS handshake message to the TLS client, and the TLS client is required to present its certificate.

Use the **no** form of this command to disable client authentication. Disabling TLS client authentication is suitable when the ASA must interoperate with CUMA client or clients such as a Web browser that are incapable of sending a client certificate.

Examples

The following example configures a TLS proxy instance with client authentication disabled:

```
ciscoasa(config)# tls-proxy mmp_tls
ciscoasa(config-tlsp)# no server authenticate-client
ciscoasa(config-tlsp)# server trust-point cuma_server_proxy
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.

server cipher-suite

To define the ciphers that the TLS proxy server can use, use the **server cipher suite** command in tls-proxy configuration mode. To use the global cipher setting, use the **no** form of this command.

server cipher-suite *cipher_list*
no server cipher-suite *cipher_list*

Syntax Description

cipher_list	Sets the ciphers to include any combination of the following: • **3des-sha1** • **aes128-sha1** • **aes256-sha1** • **des-sha1** • **null-sha1** • **rc4-sha1** Separate multiple options with spaces.

Command Default

If you do not define the ciphers the TLS proxy can use, the proxy server uses the global cipher suite defined by the **ssl cipher** command. By default, the global cipher level is medium, which means all ciphers are available except for NULL-SHA, DES-CBC-SHA, and RC4-MD5.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tls-proxy configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.8(1)	We introduced this command.

Usage Guidelines

You can now set the SSL cipher suite when the ASA acts as a TLS proxy server. Formerly, you could only set global settings for the ASA using the **ssl cipher** command.

Specify the server cipher-suite command only if you want to use a different suite than the one generally available on the ASA (the **ssl cipher** command).

To set the minimum TLS version for all SSL server connections on the ASA, see the **ssl server-version** command. The default is TLS v1.0.

Examples

The following example sets the TLS proxy server ciphers:

```
ciscoasa(config)# tls-proxy test
ciscoasa(config-tlsp)# server cipher-list aes128-sha1 aes256-sha1
```

Related Commands

Command	Description
tls-proxy	Defines a TLS proxy instance and sets the maximum number of sessions.
client cipher-list	Defines a TLS proxy client cipher suite.

server-port

To configure a AAA server port for a host, use the **server-port** command in aaa-server host mode. To remove the designated server port, use the **no** form of this command.

server-port *port-number*
no server-port *port-number*

Syntax Description

port-number	A port number in the range of 0 through 65535.

Command Default

The default server ports are as follows:

- SDI—5500
- LDAP—389
- Kerberos—88
- NT—139
- TACACS+—49

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server group	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example configures an SDI AAA server named srvgrp1 to use server port number 8888:

```
ciscoasa
(config)#
aaa-server srvgrp1 protocol sdi
ciscoasa
(config-aaa-server-group)#
aaa-server srvgrp1 host 192.168.10.10
ciscoasa
(config-aaa-server-host)#
server-port 8888
```

Related Commands

Command	Description
aaa-server host	Configures host-specific AAA server parameters.
clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

server-separator (pop3s, imap4s, smtps) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To specify a character as a delimiter between the e-mail and VPN server names, use **server-separator** command in the applicable e-mail proxy mode. To revert to the default, ":", use the no form of this command.

server-separator { *symbol* }
no server-separator

Syntax Description

symbol	The character that separates the e-mail and VPN server names. Choices are "@," (at) "|" (pipe), ":"(colon), "#" (hash), "," (comma), and ";" (semi-colon).

Command Default

The default is "@" (at).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Pop3s	• Yes	—	• Yes	—	—
Imap4s	• Yes	—	• Yes	—	—
Smtps	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5.2	This command was deprecated.

Usage Guidelines

The server separator must be different from the name separator.

Examples

The following example shows how to set a pipe (|) as the server separator for IMAP4S:

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# server-separator |
```

Related Commands

Command	Description
name-separator	Separates the e-mail and VPN usernames and passwords.

server trust-point

To specify the proxy trustpoint certificate to present during TLS handshake, use the **server trust-point** command in TLS server configuration mode.

server trust-point *proxy_trustpoint*

Syntax Description

proxy_trustpoint	Specifies the trustpoint defined by the **crypto ca trustpoint** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
TLS-proxy configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

The trustpoint can be self-signed, enrolled with a certificate authority, or from an imported credential. The **server trust-point** command has precedence over the global **ssl trust-point** command.

The **server trust-point** command specifies the proxy trustpoint certificate presented during TLS handshake. The certificate must be owned by the ASA (identity certificate). The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential.

Create TLS proxy instances for each entity that can initiate a connection. The entity that initiates the TLS connection is in the role of TLS client. Because the TLS Proxy has strict definition of client proxy and server proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

Note When you are creating the TLS proxy instance to use with the Phone Proxy, the server trustpoint is the internal Phone Proxy trustpoint created the CTL file instance. The trustpoint name is in the form*internal_PP_<ctl-file_instance_name>*

Examples

The following example shows the use of the **server trust-point** command to specify the proxy trustpoint certificate to present during TLS handshake:

```
ciscoasa
(config-tlsp)# server trust-point ent_y_proxy
```

Related Commands

Command	Description
client (tls-proxy)	Configures trustpoints, keypairs, and cipher suites for a TLS proxy instance.
client trust-point	Specifies the proxy trustpoint certificate to present during TLS handshake.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.
tls-proxy	Configures a TLS proxy instance.

server-type

To manually configure the LDAP server model, use the **server-type** command in aaa-server host configuration mode. The ASA supports the following server models:

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server, formerly named the Sun ONE Directory Server
- Generic LDAP directory servers that comply with LDAPv3 (no password management)

To disable this command, use the **no** form of this command.

server-type { **auto-detect | microsoft | sun | generic | openldap | novell** }
no server-type { **auto-detect | microsoft | sun | generic | openldap | novell** }

Syntax Description

auto-detect	Specifies that the ASA determines the LDAP server type through auto-detection.
generic	Specifies LDAP v3-compliant directory servers other than Sun and Microsoft LDAP directory servers. Password management is not supported with generic LDAP servers.
microsoft	Specifies that the LDAP server is a Microsoft Active Directory.
openldap	Specifies that the LDAP server is an OpenLDAP server.
novell	Specifies that the LDAP server is a Novell server.
sun	Specifies that the LDAP server is a Sun Microsystems JAVA System Directory Server.

Command Default

By default, auto-detection attempts to determine the server type.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	This command was added.
8.0(2)	Support for the OpenLDAP and Novell server types was added.

Usage Guidelines

The ASA supports LDAP version 3 and is compatible with the Sun Microsystems JAVA System Directory Server, the Microsoft Active Directory, and other LDAPv3 directory servers.

Note Sun—The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.

- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Generic—Password management features are not supported.

By default, the ASA auto-detects whether it is connected to a Microsoft directory server, a Sun LDAP directory server, or a generic LDAPv3 server. However, if auto-detection fails to determine the LDAP server type and if you know the server is either a Microsoft or Sun server, you can use the **server-type** command to manually configure the server as either a Microsoft or a Sun Microsystems LDAP server.

Examples

The following example, entered in aaa-server host configuration mode, configures the server type for the LDAP server ldapsvr1 at IP address 10.10.0.1. The first example configures a Sun Microsystems LDAP server.

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type sun
```

The following example specifies that the ASA use auto-detection to determine the server type:

```
ciscoasa(config)# aaa-server ldapsvr1 protocol LDAP
ciscoasa(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# server-type auto-detect
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
sasl-mechanism	Configures SASL authentication between the LDAP client and server.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

service (ctl-provider)

To specify the port to which the Certificate Trust List provider listens, use the service command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

service port *listening_port*
no service port *listening_port*

Syntax Description

port *listening_port*	Specifies the certificate to be exported to the client.

Command Default

Default port is 2444.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ctl provider configuration	• Yes	• Yes	• Tes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use the service command in CTL provider configuration mode to specify the port to which the CTL provider listens. The port must be the one listened to by the CallManager servers in the cluster (as configured under Enterprise Parameters on the CallManager administration page). The default port is 2444.

Examples

The following example shows how to create a CTL provider instance:

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.

Commands	Description
export	Specifies the certificate to be exported to the client
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

service (global)

To enable resets for denied TCP connections, use the **service** command in global configuration mode. To disable resets, use the **no** form of this command.

service { **resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside** }
no service { **resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside** }

Syntax Description

interface *interface_name*	Enables or disables resets for the specified interface.
resetinbound	Sends TCP resets for all inbound TCP sessions that attempt to transit the ASA and are denied by the ASA based on access lists or AAA settings. The ASA also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. Traffic between same security level interfaces is also affected. When this option is not enabled, the ASA silently discards denied packets. If you do not specify an interface, then this setting applies to all interfaces.
resetoutbound	Sends TCP resets for all outbound TCP sessions that attempt to transit the ASA and are denied by the ASA based on access lists or AAA settings. The ASA also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. Traffic between same security level interfaces is also affected. When this option is not enabled, the ASA silently discards denied packets. This option is enabled by default. You might want to disable outbound resets to reduce the CPU load during traffic storms, for example.
resetoutside	Enables resets for TCP packets that terminate at the least secure interface and are denied by the ASA based on access lists or AAA settings. The ASA also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. When this option is not enabled, the ASA silently discards the packets of denied packets. We recommend that you use the resetoutside keyword with interface PAT. This keyword allows the ASA to terminate the IDENT from an external SMTP or FTP server. Actively resetting these connections avoids the 30-second timeout delay. **Note** Connections are always reset for BGP and WebVPN (on the least secure interface) regardless of this option.

Command Default

By default, **service resetoutbound is** enabled for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	The **interface** keyword and the **resetoutbound** command were added.

Usage Guidelines

You might want to explicitly send resets for inbound traffic if you need to reset identity request (IDENT) connections. When you send a TCP RST (reset flag in the TCP header) to the denied host, the RST stops the incoming IDENT process so that you do not have to wait for IDENT to time out. Waiting for IDENT to time out can cause traffic to slow because outside hosts keep retransmitting the SYN until the IDENT times out, so the **service resetinbound** command might improve performance.

Examples

The following example disables outbound resets for all interfaces except for the inside interface:

```
ciscoasa(config)# no
            service resetoutbound
ciscoasa(config)# service resetoutbound interface inside
```

The following example enables inbound resets for all interfaces except for the DMZ interface:

```
ciscoasa(config)# service resetinbound
ciscoasa(config)# no
            service resetinbound interface dmz
```

The following example enables resets for connections that terminate on the outside interface:

```
ciscoasa(config)# service resetoutside
```

Related Commands

Command	Description
show running-config service	Displays the service configuration.

service (object service)

To define the protocol and optional attributes for a service object, use the **service** command in object service configuration mode. Use the **no** form of this command to remove the definition.

service { *protocol* | { **tcp | udp | sctp** } [**source** *operator number*] [**destination** *operator number*] | { **icmp | icmp6** } [*icmp_type* [*icmp_code*]] }
no service { *protocol* | { **tcp | udp | sctp** } [**source** *operator number*] [**destination** *operator number*] | { **icmp | icmp6** } [*icmp_type* [*icmp_code*]] }

Syntax Description

destination *operator number*	(Optional; **tcp** , **udp** , **sctp** only.) Specifies the destination port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **eq** —Equals the port number. • **gt** —Greater than the port number. • **lt** —Less than the port number. • **neq** —Not equal to the port number. • **range** —A range of ports. Specify two numbers separated by a space, such as **range 1024 4500** .
{ **icmp** | **icmp6** } [*icmp_type* [*icmp_code*]]	Specifies that the service type is for ICMP or ICMP version 6 connections. You can optionally specify the ICMP type by name or number, between 0 and 255. (For available optional ICMP type names, see the CLI help.) If you specify a type, you can optionally include an ICMP code, between 1 and 255.
protocol	Identifies the protocol name or number, between 0 and 255. For a list of supported names, see the CLI help.
sctp	Specifies that the service type is for Stream Control Transmission Protocol (SCTP) connections.
source *operator number*	(Optional; **tcp** , **udp** , **sctp** only.) Specifies the source port name or number, between 0 and 65535. For a list of supported names, see the CLI help. The operators are the same as those for **destination** .
tcp	Specifies that the service type is for TCP connections.
udp	Specifies that the service type is for UDP connections.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.0(1)	Support for ICMP code was added.
9.5(2)	Support for SCTP was added.

Usage Guidelines

You can use service objects by name in other parts of your configuration, for example ACLs (the **access-list** command) and NAT (the **nat** command).

If you configure an existing service object with a different protocol and port, the new configuration replaces the existing protocol and port with the new ones.

Examples

The following example shows how to create a service object for SSH traffic:

```
ciscoasa(config)# object service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
```

The following example shows how to create a service object for EIGRP traffic:

```
ciscoasa(config)# object service EIGRP
ciscoasa(config-service-object)# service eigrp
```

The following example shows how to create a service object for traffic coming from port 0 through 1024 to HTTPS:

```
ciscoasa(config)# object service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
object-group service	Configures a service object.
show running-config object service	Shows the current service object configuration.

service call-home

To enable the Call Home service, use the **service call-home** command in global configuration mode. To disable the Call Home service, use the **no** form of this command.

service call-home
no service call-home

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the service Call Home command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added.

Examples

The following example shows how to enable the Call Home service:

```
ciscoasa(config)# service call-home
```

The following example shows how to disable the Call Home service:

```
hostname(config)# no service call-home
```

Related Commands

Command	Description
call-home (global configuration)	Enters Call Home configuration mode.
call-home test	Manually sends a Call Home test message.
show call-home	Displays Call Home configuration information.

service-module

To adjust how quickly the system will determine that a service module is no longer responding, use the **service-module** command in global configuration mode. To return to the default settings, use the **no** form of this command.

service-module { *module_id* | **all** } { **keepalive-counter | keepalive-timeout** } *value*
no service-module { *module_id* | **all** } { **keepalive-counter | keepalive-timeout** } *value*

Syntax Description

{ *module_id* | **all** }	Specifies the module whose keepalive values you are adjusting. Specify **all** to adjust them for all modules. Use ? to determine the module IDs that are valid for your system. These are typically: • **1** for the module in the first slot. • **sfr** for the ASA FirePOWER module.
keepalive-counter *value*	The maximum number of keepalives that can be sent without a response before the module is considered down, from 1-12.
keepalive-timeout *value*	The length of time between sending keepalive messages, from 4-16 seconds.

Command Default

Default count is 6, default timeout is 4.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.12(3)	This command was added.

Usage Guidelines

The system periodically checks the service module health status by sending control plane keepalive messages. If there are communication delays caused by high CPU, the system might not get a response quickly enough, and conclude that it had not received a response from the module. The system will then declare the module to be down, when it is in fact functioning normally, and close the communication channel. When configured for high availability, the system will then fail over to the backup unit due to service card failure. If this happens frequently in your setup, extend the keepalive time or count to give the system more time to declare the module failed.

Examples

The following example shows how to change the keepalive count and timeout:

```
ciscoasa(config)# service-module all keepalive-count 10

ciscoasa(config)# service-module all keepalive-timeout 8
```

service-object

To add a service or service object to a service object group that is not pre-defined as TCP, UDP, or TCP-UDP, use the service-object command in object-group service configuration mode. To remove a service, use the **no** form of this command.

service-object { *protocol* | { **tcp | udp |tcp-udp | sctp** } [**source** *operator number*] [**destination** *operator number*] | { **icmp | icmp6** } [*icmp_type* [*icmp_code*]] | **object** *name* }
no service-object { *protocol* | { **tcp | udp |tcp-udp | sctp** } [**source** *operator number*] [**destination** *operator number*] | { **icmp | icmp6** } [*icmp_type* [*icmp_code*]] | **object** *name* }

Syntax Description

destination *operator number*	(Optional; **tcp** , **udp** , **tcp-udp** , **sctp** only.) Specifies the destination port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **eq** —Equals the port number. • **gt** —Greater than the port number. • **lt** —Less than the port number. • **neq** —Not equal to the port number. • **range** —A range of ports. Specify two numbers separated by a space, such as **range 1024 4500** .
{ **icmp** | **icmp6** } [*icmp_type* [*icmp_code*]]	Specifies that the service type is for ICMP or ICMP version 6 connections. You can optionally specify the ICMP type by name or number, between 0 and 255. (For available optional ICMP type names, see the CLI help.) If you specify a type, you can optionally include an ICMP code, between 1 and 255.
object *name*	Adds the named object or group to the object.
protocol	Identifies the protocol name or number, between 0 and 255. For a list of supported names, see the CLI help.
sctp	Specifies that the service type is for Stream Control Transmission Protocol (SCTP) connections.
source *operator number*	(Optional; **tcp** , **udp** , **tcp-udp** , **sctp** only.) Specifies the source port name or number, between 0 and 65535. For a list of supported names, see the CLI help. The operators are the same as those for **destination** .
tcp	Specifies that the service type is for TCP connections.
tcp-udp	Specifies that the service type is for TCP or UDP connections.
udp	Specifies that the service type is for UDP connections.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object-group service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(1)	This command was added.
8.3(1)	The **object** keyword was added to support service objects (the **object service** command).
9.0(1)	Support for ICMP code was added.
9.5(2)	Support for SCTP was added.

Usage Guidelines

When you create a service object group with the **object-group service** command, and you do not pre-define the protocol type for the whole group, then you can add multiple services and service objects to the group of various protocols, including ports, using the **service-object** command. When you create a service object group for a specific protocol type using the **object-group service** [**tcp** | **udp** | **tcp-udp**] command, then you can only identify the destination ports for the object group using the **port-object** command.

Examples

The following example shows how to add both TCP and UDP services to a service object group:

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

The following example shows how to add multiple service objects to a service object group:

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh
hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp
hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# service-object object SSH
ciscoasa(config-service-object-group)# service-object object EIGRP
ciscoasa(config-service-object-group)# service-object object HTTPS
```

Related Commands

Command	Description
clear configure object-group	Removes all the **object-group** commands from the configuration.

Command	Description
network-object	Adds a network object to a network object group.
object service	Adds a service object.
object-group	Defines object groups to optimize your configuration.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

service password-recovery

To enable password recovery, use the **service password-recovery** command in global configuration mode. To disable password recovery, use the **no** form of this command. Password recovery is enabled by default, but you might want to disable it to ensure that unauthorized users cannot use the password recovery mechanism to compromise the ASA.

service password-recovery
no service password-recovery

Syntax Description

This command has no arguments or keywords.

Command Default

Password recovery is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

On the ASA 5500 series adaptive security appliance, if you forget the passwords, you can boot the ASA into ROMMON by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then set the ASA to ignore the startup configuration by changing the configuration register (see the **config-register** command). For example if your configuration register is the default 0x1, then change the value to 0x41 by entering the **confreg 0x41** command. After reloading the ASA, it loads a default configuration, and you can enter privileged EXEC mode using the default passwords. Then load the startup configuration by copying it to the running configuration and reset the passwords. Finally, set the ASA to boot as before by setting the configuration register to the original setting. For example, enter the **config-register 0x1** command in global configuration mode.

On the PIX 500 series security appliance, boot the ASA into monitor mode by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then download the PIX password tool to the ASA, which erases all passwords and **aaa authentication** commands.

On the ASA 5500 series adaptive security appliance, the **no service password-recovery** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the ASA prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the ASA reloads. Because password recovery depends on using ROMMON and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command appears in the configuration file for informational purposes only; when you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the ASA is configured to ignore the startup configuration at startup (in preparation for password recovery), then the ASA changes the setting to boot the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

On the PIX 500 series security appliance, the **no service password-recovery** command forces the PIX password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the ASA reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available.

Examples

The following example disables password recovery for the ASA 5500 series:

```
ciscoasa(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery mechanism
 and disabled access to ROMMON. The only means of recovering from lost or forgotten passwords
 will be for ROMMON to erase all file systems including configuration files and images. You
 should make a backup of your configuration and have a mechanism to restore images from the
 ROMMON command line.
```

The following example for the ASA 5500 series shows when to enter ROMMON at startup and how to complete a password recovery operation.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
ciscoasa> enable
Password:
```

```
ciscoasa# configure terminal
ciscoasa(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
ciscoasa(config)# enable password
 NewPassword
ciscoasa(config)# config-register 0x1
```

Related Commands

Command	Description
config-register	Sets the ASA to ignore the startup configuration when it reloads.
enable password	Sets the enable password.
password	Sets the login password.

service-policy (class)

To apply a hierarchical policy map under another policy map, use the **service-policy** command in class configuration mode. To disable the service policy, use the **no** form of this command. Hierarchical policies are supported only for QoS traffic shaping when you want to perform priority queuing on a subset of shaped traffic.

service-policy *policymap_name*
no service-policy *policymap_name*

Syntax Description

policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map that includes the **priority** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.

Usage Guidelines

Hierarchical priority queuing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used (the **priority-queue** command).

For hierarchical priority-queuing, perform the following tasks using Modular Policy Framework:

1.class-map—Identify the traffic on which you want to perform priority queuing.

2.policy-map (for priority queuing)—Identify the actions associated with each class map.

a.class—Identify the class map on which you want to perform actions.

b.priority—Enable priority queuing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.

3.policy-map (for traffic shaping)—Identify the actions associated with the **class-default** class map.

a.class class-default—Identify the **class-default** class map on which you want to perform actions.

b.shape—Apply traffic shaping to the class map.

c.service-policy—Call the priority queuing policy map in which you configured the **priority** command so you can apply priority queuing to a subset of shaped traffic.

4.service-policy—Assigns the policy map to an interface or globally.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
ciscoasa
(config)#
class-map TG1-voice
ciscoasa
(config-cmap)#
match tunnel-group tunnel-grp1
ciscoasa
(config-cmap)#
match dscp ef
ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class
 TG1-voice
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class
 class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy
ciscoasa
(config-pmap-c)#
service-policy shape_policy
 interface outside
```

Related Commands

Command	Description
class (policy-map)	Identifies a class map for a policy map.
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
policy-map	Identifies actions to perform on class maps.
priority	Enables priority queuing.
service-policy (global)	Applies a policy map to an interface.
shape	Enables traffic shaping.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

service-policy (global)

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in global configuration mode. To disable the service policy, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface.

service-policy *policymap_name* [**global | interface** *intf*] [**fail-close**]
no service-policy *policymap_name* [**global | interface** *intf*] [**fail-close**]

Syntax Description

fail-close	Generates a syslog (767001) for IPv6 traffic that is dropped by application inspections that do not support IPv6 traffic. By default, syslogs are not generated.
global	Applies the policy map to all interfaces.
interface *intf*	Applies the policy map to a specific interface.
policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map, and not an inspection policy map (**policy-map type inspect**).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	The **fail-close** keyword was added.

Usage Guidelines

To enable the service policy, use the Modular Policy Framework:

1. **class-map** —Identify the traffic on which you want to perform priority queuing.
2. **policy-map** —Identify the actions associated with each class map.

a. **class** —Identify the class map on which you want to perform actions.

b. *commands for supported features* —For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the CLI configuration guide for more details about the commands available for each feature.

3. **service-policy** —Assigns the policy map to an interface or globally.

Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with inspections, and an interface policy with TCP normalization, then both inspections and TCP normalization are applied to the interface. However, if you have a global policy with inspections, and an interface policy with inspections, then only the interface policy inspections are applied to that interface.

By default, the configuration includes a global policy that matches all default application inspection traffic and applies inspection to the traffic globally. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one.

The default service policy includes the following command:

```
service-policy global_policy global
```

Examples

The following example shows how to enable the inbound_policy policy map on the outside interface:

```
ciscoasa(config)# service-policy inbound_policy interface outside
```

The following commands disable the default global policy, and enables a new one called new_global_policy on all other ASA interfaces:

```
ciscoasa(config)# no service-policy global_policy global
ciscoasa(config)# service-policy new_global_policy global
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
service-policy (class)	Applies a hierarchical policy under another policy map.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

service sw-reset-button

To enable the reset button on the ASA 5506-X, 5508-X, and 5516-X, use the **service sw-reset-button** command in global configuration mode. To disable the reset button, use the **no** form of this command.

service sw-reset-button
no service sw-reset-button

Syntax Description

This command has no arguments or keywords.

Command Default

By default, **service sw-reset-button** is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	Command added.

Usage Guidelines

The reset button is a small recessed button on the rear panel that if pressed for longer than three seconds resets the ASA to its default "as-shipped" state following the next reboot. Configuration variables are reset to factory default. However, the flash is not erased, and no files are removed.

Examples

The following example enables the software reset button:

```
ciscoasa(config)# service sw-reset-button
ciscoasa(config)# show sw-reset-button
Software Reset Button is configured.
```

The following example disables the software reset button:

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button
Software Reset Button is not configured.
```

Related Commands

Command	Description
show running-config service	Displays the service configuration.

service telemetry

When the telemetry data service is enabled, information about the device information, CPU/memory/disk/bandwidth usage, license usage, configured feature list, cluster/failover information, and the alike on the customer ASA devices are sent to Cisco Security Service Exchange (SSE) through Secure Firewall eXtensible Operating System (FXOS). Use the **service telemetry** command in global configuration mode to enable the service. To disable the telemetry service, use the **no** form of this command.

service telemetry
no service telemetry

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the service telemetry command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The ASA telemetry service is supported in the SSPXRU (FP9300 and FP4100) platforms running the ASA application. This command is used to control per blade telemetry support. To control per chassis telemetry support, you need to enable it in the FXOS/chassis manager.

Examples

The following example shows how to enable the telemetry service:

```
ciscoasa(config)# service telemetry
```

The following example shows how to disable the telemetry service:

```
hostname(config)# no service telemetry
```

Related Commands

Command	Description
show telemetry	Displays the past 100 events related to telemetry configuration and activities. Also, displays the last sent telemetry data and samples in JSON format.

session

To establish a Telnet session from the ASA to a module, such as an IPS SSP or a CSC SSM, to access the module CLI, use the **session** command in privileged EXEC mode.

session*id*

Syntax Description

id	Specifies the module ID: • Physical module—**1** (for slot number 1) • Software module, ASA FirePOWER—**sfr** • Software module, IPS—**ips** • Software module, ASA CX—**cxsc**

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.6(1)	The **ips** module ID for the IPS SSP software module was added.
9.1(1)	Support for the ASA CX module was added (the **cxsc** keyword).
9.2(1)	Support for the ASA FirePOWER module was added (the **sfr** keyword).

Usage Guidelines

This command is only available when the module is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6,** then the **x** key.

Note that the **session 1** command does not work with the following hardware modules:

- ASA CX
- ASA FirePOWER

Examples

The following example sessions to a module in slot 1:

```
ciscoasa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Related Commands

Command	Description
debug session-command	Shows debugging messages for sessions.

session console

To establish a virtual console session from the ASA to a software module, such as an IPS SSP software module, use the **session console** command in privileged EXEC mode. This command might be useful if you cannot establish a Telnet session using the **session** command because the control plane is down.

session *id* **console**

Syntax Description

id	Specifies the module ID: • ASA FirePOWER module—**sfr** • IPS module—**ips** • ASA CX module—**cxsc** • ASA 5506W-X wireless access point—**wlan**

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	This command was added.
9.1(1)	Support for the ASA CX module was added (the **cxsc** keyword).
9.2(1)	Support for the ASA FirePOWER module was added (the **sfr** keyword).
9.4(1)	Support for the ASA 5506W-X wireless access point (the **wlan** keyword) was added.

Usage Guidelines

To end a session, enter **Ctrl-Shift-6,** then the **x** key.

Do not use this command in conjunction with a terminal server where **Ctrl-Shift-6, x** is the escape sequence to return to the terminal server prompt. **Ctrl-Shift-6, x** is also the sequence to escape the module console and return to the ASA prompt. Therefore, if you try to exit the module console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the ASA, the module console session is still active; you can never exit to the ASA prompt. You must use a direct serial connection to return the console to the ASA prompt.

Use the **session** command instead.

Examples

The following example creates a console session to the IPS module:

```
ciscoasa# session ips console
Establishing console session with slot 1
Opening console session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.
sensor login: service
Password: test
```

The following example creates a console session to the wireless access point:

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is ‘CTRL-^X’
ap>
```

Related Commands

Command	Description
session	Initiates a Telnet session to a module.
show module log console	Displays console log information.

session do

To establish a Telnet session and perform a command from the ASA to a module, use the **session do** command in privileged EXEC mode.

session *id* **do** *command*

Syntax Description

id	Specifies the module ID: • Physical module—**1** (for slot number 1) • Software module, ASA FirePOWER—**sfr** • Software module, IPS—**ips** • Software module, ASA CX—**cxsc**
command	Performs a command on the module. Supported commands include: • **setup host ip** *ip_address*/*mask*,*gateway_ip* —Sets the management IP address and gateway. • **get-config**—Gets the module configuration. • **password-reset**—Resets the module password to the default.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.1(1)	This command was added.
8.6(1)	The **ips** module ID for the IPS SSP software module was added.
8.4(4.1)	Support for the ASA CX module was added.
9.2(1)	Support for the ASA FirePOWER module, including the **sfr** keyword was added.

Usage Guidelines

This command is only available when the module is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6,** then the **X** key.

Examples

The following example sets the management IP address to 10.1.1.2/24, with a default gateway of 10.1.1.1:

```
ciscoasa# session 1 do setup host ip 10.1.1.2/24,10.1.1.1
```

Related Commands

Command	Description
debug session-command	Shows debugging messages for sessions.

session ip

To configure logging IP addresses for the module, such as an IPS SSP or a CSC SSM, use the **session ip** command in privileged EXEC mode.

session *id* **ip** { **address** *address mask* | **gateway** *address* }

Syntax Description

id	Specifies the module ID: • Physical module—**1** (for slot number 1) • Software module, IPS—**ips**
address *address*	Sets the syslog server address.
gateway *address*	Sets the gateway to the syslog server.
mask	Sets the subnet mask.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.1(1)	This command was added.
8.4(4.1)	Support for the ASA CX module was added.
8.6(1)	The **ips** module ID for the IPS SSP software module was added.

Usage Guidelines

This command is only available when the module is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6,** then the **X** key.

Examples

The following example sessions to a module in slot 1:

```
ciscoasa# session 1 ip
address
```

Related Commands

Command	Description
debug session-command	Shows debugging messages for sessions.

set adaptive-interface cost

To set the output interface based on the adaptive interface cost on the candidate interfaces, use the **set adaptive-interface cost** command in route map configuration mode

set adaptive-interface cost *interface_list*

Syntax Description

interface_list	A space-separated list of interface names. The egress interface is selected from these interfaces.

Command Default

No default values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.

Usage Guidelines

Set the cost of the interface in the interface configuration using the **policy-route cost** command. The default cost is 0, so you can use adaptive interface cost even without setting an explicit cost value.

If the costs of the interfaces are the same, it is an active-active configuration and packets are load-balanced (round-robin) on the egress interfaces. If the costs are different, the interface with the lowest cost is selected. Interfaces are considered only if they are up.

For example, by setting the same cost on 2 WAN links, you can load balance the traffic across those links to perhaps improve performance. However, if one WAN link has higher bandwidth than the other, you can set the higher bandwidth link's cost to 1, and the lower bandwidth link to 2, so that the lower bandwidth link is used only if the higher bandwidth link is down.

After you configure the route map with this command, you must apply it to the ingress interfaces using the **policy-route route-map** command.

Example

The following example sets output1 and output2 as the candidate egress interfaces based on their cost.

```
ciscoasa(config)# route-map mymap 10
ciscoasa(config-route-map)# match ip address DIA_traffic
ciscoasa(config-route-map)# set adaptive-interface cost output1 output2
```

set as-path

To modify an autonomous system path for BGP routes, use the set as-path command in route-map configuration mode. To not modify the autonomous system path, use the no form of this command.

set as-path { **tag** | **prepend** *as-path-string* }
no set as-path { **tag** | **prepend** *as-path-string* }

Syntax Description

as-path-string	Number of an autonomous system to prepend to the AS_PATH attribute. The range of values for this argument is any valid autonomous system number from 1 to 65535. Multiple values can be entered; up to 10 AS numbers can be entered. For more details about autonomous system number formats, see the router bgp command.
prepend	Appends the string following the keyword prepend to the autonomous system path of the route that is matched by the route map. Applies to inbound and outbound BGP route maps.
tag	Converts the tag of a route into an autonomous system path. Applies only when redistributing routes into BGP.

Command Default

An autonomous system path is not modified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The only global BGP metric available to influence the best path selection is the autonomous system path length. By varying the length of the autonomous system path, a BGP speaker can influence the best path selection by a peer further away.

By allowing you to convert the tag into an autonomous system path, the set as-path tag variation of this command modifies the autonomous system length. The set as-path prepend variation allows you to "prepend" an arbitrary autonomous system path string to BGP routes. Usually the local autonomous system number is prepended multiple times, increasing the autonomous system path length.

Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command followed by the clear bgp * command to perform a hard reset of all current BGP sessions.

Examples

The following example converts the tag of a redistributed route into an autonomous system path:

```
ciscoasa(config)# route-map set-as-path-from-tag
ciscoasa(config-route-map)# set as-path tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
 ciscoasa(config-router-af)# redistribute ospf 109 route-map set-as-path-from-tag
```

The following example prepends 100 100 100 to all the routes that are advertised to 10.108.1.1:

```
ciscoasa(config)# route-map set-as-path
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set as-path prepend 100 100 100
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 route-map set-as-path out
```

Related Commands

Command	Description
clear bgp	Resets BGP connections using hard or soft reconfiguration.
bgp asnotation dot	Changes the default display and regular expression match format of Border Gateway Protocol (BGP) 4-byte autonomous system numbers from asplain format (decimal values) to dot notation.

set automatic-tag

To automatically compute the tag value, use the **set automatic-tag** command in route-map configuration mode. To disable this function, use the **no** form of this command.

set automatic-tag
no set automatic-tag

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You must have a match clause (even if it points permit everything) if you want to set tags.

Use the **route-map** global configuration command and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example configures the ASA software to automatically compute the tag value for the Border Gateway Protocol (BGP) learned routes:

```
ciscoasa(config-route-map)# route-map tag
ciscoasa(config-route-map)# match as-path 10
iscoasa(config-route-map)# set automatic-tag
ciscoasa(config-route-map)# router bgp 100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# table-map tag
```

set community

To set the BGP communities attribute, use the set community route map configuration command. To delete the entry, use the no form of this command.

set community { *community-number* [**additive**] | [*well-known-community*] [**additive**] | **none** }
no set community

Syntax Description

additive	(Optional) Adds the community to the already existing community.
community-number	Specifies that community number. Valid values are from 1 to 4294967200, no-export, or no-advertise.
none	(Optional) Removes the community attribute from the prefixes that pass the route map.
well-known-community	(Optional) Well-known communities can be specified by using the following keywords: • **internet** • **local-as** • **no-advertise** • **no-export**

Command Default

No BGP communities attributes exist.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You must have a match clause (even if it points to a “permit everything” list) if you want to set tags.

Use the route-map global configuration command, and the match and set route map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

In the following example, routes that pass the autonomous system path access list 1 have the community set to 109. Routes that pass the autonomous system path access list 2 have the community set to no-export (these routes will not be advertised to any external BGP [eBGP] peers).

```
ciscoasa(config-route-map)# set community 10
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set community 109
ciscoasa(config-route-map)# set community 20
ciscoasa(config-route-map)# match as-path 2
ciscoasa(config-route-map)# set community no-export
```

Related Commands

Command	Description
match as-path	Match a BGP autonomous system path that is specified by an access list.

set connection

To specify connection limits within a policy map for a traffic class, use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection { [**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**syn-cookie-mss** *n*] [**random-sequence-number** { **enable | disable** }] }
no set connection { [**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**syn-cookie-mss** *n*] [**random-sequence-number** { **enable | disable** }] }

Syntax Description

conn-max *n*	(TCP, UDP, SCTP.) Sets the maximum number of simultaneous connections that are allowed, between 0 and 2000000. The default is 0, which allows unlimited connections. For example, if two servers are configured to allow simultaneous connections, the connection limit is applied to each configured server separately. For TCP connections, this applies to established connections only. When configured under a class, this argument restricts the maximum number of simultaneous connections that are allowed for the entire class. In this case, one attack host can consume all the connections and leave none of the rest of the hosts matched in the access list under the class.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic TCP connections allowed, between 0 and 2000000. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic TCP connections allowed per client, between 0 and 2000000. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the ASA. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	(TCP, UDP, SCTP.) Sets the maximum number of simultaneous connections allowed per client, between 0 and 2000000. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the ASA. For TCP connections, this includes established, half-open, and half-closed connections. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for each host that is matched through an access list under the class.

random-sequence-number { **enable** | **disable** }	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.
syn-cookie-mss *n*	Sets the server maximum segment size (MSS) for SYN-cookie generation for embryonic connections upon reaching the embryonic connections limit, from 48 to 65535 . The default is 1380. This setting is meaningful only if you configure **set connection embryonic-conn-max** or **per-client-embryonic-max**.

Command Default

For the **conn-max** , **embryonic-conn-max** , **per-client-embryonic-max** , and **per-client-max** parameters, the default value of *n* is 0, which allows unlimited connections.

Sequence number randomization is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The **per-client-embryonic-max** and **per-client-max** keywords were added.
8.0(2)	This command is now available for a Layer 3/4 management class map, for to-the-ASA management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.
9.0(1)	The maximum number of connections was increased from 65535 to 2000000.
9.5(2)	The **conn-max** and **per-client-max** keywords now apply to SCTP as well as TCP and UDP.
9.16(1)	The **syn-cookie-mss** keyword was added.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command (for through traffic) or **class-map type management** command (for management traffic). Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the CLI configuration guide.

Note Depending on the number of CPU cores on your ASA model, the maximum concurrent and embryonic connections may exceed the configured numbers due to the way each core manages connections. In the worst case scenario, the ASA allows up to *n* -1 extra connections and embryonic connections, where *n* is the number of cores. For example, if your model has 4 cores, if you configure 6 concurrent connections and 4 embryonic connections, you could have an additional 3 of each type. To determine the number of cores for your model, enter the **show cpu core** command.

TCP Intercept Overview

Limiting the number of embryonic connections protects you from a DoS attack. The ASA uses the per-client limits and the embryonic connection limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the ASA receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

TCP Sequence Randomization

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The ASA randomizes the ISN of the TCP SYN passing in both the inbound and outbound directions.

Randomizing the ISN of the protected host prevents an attacker from predicting the next ISN for a new connection and potentially hijacking the new session.

TCP initial sequence number randomization can be disabled if required. For example:

- If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic.
- If you use eBGP multi-hop through the ASA, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- You use a WAAS device that requires the ASA not to randomize the sequence numbers of connections.

Examples

The following is an example of the use of the **set connection** command configure the maximum number of simultaneous connections as 256 and to disable TCP sequence number randomization:

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
ciscoasa(config-pmap-c)#
```

You can enter this command with multiple parameters or you can enter each parameter as a separate command. The ASA combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
ciscoasa(config-pmap-c)# set connection conn-max 600
ciscoasa(config-pmap-c)# set connection embryonic-conn-max 50
```

The output of the **show running-config policy-map** command would display the result of the two commands in a single, combined command:

```
set connection conn-max 600 embryonic-conn-max 50
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Removes all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy-map configurations.
show service-policy	Displays service policy configuration. Use the **set connection** keyword to view policies that include the **set connection** command.

set connection advanced-options

To configure advanced connection settings, use the **set connection advanced-options** command in class configuration mode. To remove the options, use the **no** form of this command.

set connection advanced-options { *tcp_mapname* | **tcp-state-bypass | sctp-state-bypass | flow-offload** }
no set connection advanced-options { *tcp_mapname* | **tcp-state-bypass | sctp-state-bypass | flow-offload** }

Syntax Description

flow-offload	Identify matching flows as eligible for off-loading from the ASA and switched directly in the NIC. This provides improved performance for large data flows in data centers. Flow off-load is available for the Firepower 9300 series running FXOS 1.1.3+, or the Firepower 4100 series running FXOS 1.1.4+, or the Secure Firewall 3100 series. You must also enable flow off-loading before this option works. Use the **flow-offload enable** command.
sctp-state-bypass	Implements SCTP State Bypass to turn off SCTP stateful inspection. SCTP traffic is not validated for protocol conformance.
tcp_mapname	Name of a TCP map created by the **tcp-map** command. Use this option to customize TCP normalization.
tcp-state-bypass	Bypass TCP state checking if you use asymmetrical routing in your network. See the Usage section below for detail information and guidelines for using TCP State Bypass.

Command Default

No default behavior or values. No options are enabled by default, although all TCP Normalizer options (within a TCP map) have default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	The **tcp-state-bypass** keyword was added.
9.5(2)	The **sctp-state-bypass** keyword was added.
9.5(2)	The **flow-offload** keyword was added. The option also requires FXOS 1.1.3+, and is available for the Firepower 9300 series.

Release	Modification
9.6(1)	Flow offload support was added for the Firepower 4100 series running FXOS 1.1.4+.
9.19(1)	Support added for the Secure Firewall 3100.

Usage Guidelines

To customize TCP normalization with a TCP map, use the Modular Policy Framework:

1. **tcp-map** —Identify the TCP normalization actions if you intend to modify them.
2. **class-map** —Identify the traffic on which you want to perform TCP normalization actions.
3. **policy-map** —Identify the actions associated with the class map.

a. **class** —Identify the class map on which you want to perform actions.

b. **set connection advanced options** —Apply a TCP map or another option to the class map.

4. **service-policy** —Assigns the policy map to an interface or globally.

TCP State Bypass: Allowing Outbound and Inbound Flows through Separate Devices

By default, all traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. The ASA maximizes the firewall performance by checking the state of each packet (is this a new connection or an established connection?) and assigning it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection).

TCP packets that match existing connections in the fast path can pass through the ASA without rechecking every aspect of the security policy. This feature maximizes performance. However, the method of establishing the session in the fast path using the SYN packet, and the checks that occur in the fast path (such as TCP sequence number), can stand in the way of asymmetrical routing solutions: both the outbound and inbound flow of a connection must pass through the same ASA.

For example, a new connection goes to ASA 1. The SYN packet goes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets of this connection go through ASA 1, then the packets will match the entry in the fast path, and are passed through. But if subsequent packets go to ASA 2, where there was not a SYN packet that went through the session management path, then there is no entry in the fast path for the connection, and the packets are dropped.

If you have asymmetric routing configured on upstream routers, and traffic alternates between two ASAs, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic much as it treats a UDP connection: when a non-SYN packet matching the specified networks enters the ASA, and there is not a fast path entry, then the packet goes through the session management path to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

Unsupported Features for TCP State Bypass

The following features are not supported when you use TCP state bypass:

- Application inspection—Application inspection requires both inbound and outbound traffic to go through the same ASA, so application inspection is not supported with TCP state bypass.
- AAA authenticated sessions—When a user authenticates with one ASA, traffic returning via the other ASA will be denied because the user did not authenticate with that ASA.
- TCP Intercept, maximum embryonic connection limit, TCP sequence number randomization—The ASA does not keep track of the state of the connection, so these features are not applied.

- TCP normalization—The TCP normalizer is disabled.
- SSM functionality—You cannot use TCP state bypass and any application running on an SSM, such as IPS or CSC.

NAT Guidelines for TCP State Bypass

Because the translation session is established separately for each ASA, be sure to configure static NAT on both ASAs for TCP state bypass traffic; if you use dynamic NAT, the address chosen for the session on ASA 1 will differ from the address chosen for the session on ASA 2.

Connection Timeout Guidelines for TCP State Bypass

Starting with release 9.10(1), if there is no traffic on a given connection for 2 minutes, the connection times out. You can override this default using the **set connection timeout idle** command. Normal TCP connections timeout by default after 60 minutes. In releases prior to 9.10(1), the TCP state bypass connections use the global timeout value of 60 minutes.

Examples

The following example shows the use of the **set connection advanced-options** command to specify the use of a TCP map named localmap:

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config-cmap)# exit
ciscoasa(config)# tcp-map localmap
ciscoasa(config)# policy-map global_policy global
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection advanced-options localmap
ciscoasa(config-pmap-c)#
```

The following is an example configuration for TCP state bypass:

```
ciscoasa(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any
ciscoasa(config)# class-map tcp_bypass
ciscoasa(config-cmap)# description "TCP traffic that bypasses stateful firewall"
ciscoasa(config-cmap)# match access-list tcp_bypass
ciscoasa(config-cmap)# policy-map tcp_bypass_policy
ciscoasa(config-pmap)# class tcp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options tcp-state-bypass
ciscoasa(config-pmap-c)# service-policy tcp_bypass_policy interface outside
```

The following is an example configuration for SCTP state bypass:

```
ciscoasa(config)# access-list sctp_bypass extended permit sctp
            10.1.1.0 255.255.255.224 any
ciscoasa(config)# class-map sctp_bypass
ciscoasa(config-cmap)# description "SCTP traffic that bypasses stateful inspection"
ciscoasa(config-cmap)# match access-list sctp_bypass
ciscoasa(config-cmap)# policy-map sctp_bypass_policy
ciscoasa(config-pmap)# class sctp_bypass
ciscoasa(config-pmap-c)# set connection advanced-options sctp-state-bypass
ciscoasa(config-pmap-c)# service-policy sctp_bypass_policy interface outside
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
flow-offload	Enables flow offload.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
set connection timeout	Sets the connection timeouts.
show running-config policy-map	Display all current policy-map configurations.
tcp-map	Creates a TCP map.

set connection decrement-ttl

To decrement the time to live value within a policy map for a traffic class, use the **set connection decrement-ttl** command in class configuration mode. To not decrement the time to live, use the **no** form of this command.

set connection decrement-ttl
no set connection decrement-ttl

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA does not decrement the time to live.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(2)	This command was added.

Usage Guidelines

This command, along with the **icmp unreachable** command, is required to allow a traceroute through the ASA that shows the ASA as one of the hops.

If you decrement time to live, packets with a TTL of 1 will be dropped, but a connection will be opened for the session on the assumption that the connection might contain packets with a greater TTL. Note that some packets, such as OSPF hello packets, are sent with TTL = 1, so decrementing time to live can have unexpected consequences.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
icmp unreachable	Controls the rate at which ICMP unreachables are allowed through the ASA.

Command	Description
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Displays service policy configuration.

set connection timeout

To specify connection timeouts within a policy map for a traffic class, use the **set connection timeout** command in class configuration mode. To remove the timeout, use the **no** form of this command.

set connection timeout { [**embryonic** *hh* **:** *mm* **:** *ss*] [**idle** *hh* **:** *mm* **:** *ss* [**reset**]] [**half-closed** *hh* **:** *mm* **:** *ss*] [**dcd** [*retry_interval* [*max_retries*]]] }
no set connection timeout { [**embryonic** *hh* **:** *mm* **:** *ss*] [**idle** *hh* **:** *mm* **:** *ss*] [**reset**] [**half-closed** *hh* **:** *mm* **:** *ss*] [**dcd** [*retry_interval* [*max_retries*]]] }

Syntax Description

dcd [*retry_interval* [*max_retries*]]	Enables dead connection detection (DCD). DCD detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist. After a TCP connection times out, the ASA sends DCD probes to the end hosts to determine the validity of the connection. If one of the end hosts fails to respond after the maximum retries are exhausted, the ASA frees the connection. If both end hosts respond that the connection is valid, the ASA updates the activity timeout to the current time and reschedules the idle timeout accordingly. When operating in transparent firewall mode, you must configure static routes for the endpoints. You cannot use DCD in a cluster until version 9.13(1). You can configure the following optional values: • *retry_interval* —Time duration in *hh* **:** *mm* **:** *ss* format to wait after each unresponsive DCD probe before sending another probe, between 0:0:1 and 24:0:0. The default is 0:0:15. For systems that are operating in a cluster or high-availability configuration, we recommend that you do not set the interval to less than one minute (0:1:0). If the connection needs to be moved between systems, the changes required take longer than 30 seconds, and the connection might be deleted before the change is accomplished. • *max_retries* —Sets the number of consecutive failed retries for DCD before declaring the connection as dead. The minimum value is 1 and the maximum value is 255. The default is 5.
embryonic *hh* **:** *mm* **:** *ss*	Sets the timeout period until a TCP embryonic (half-open) connection is closed, between 0:0:5 and 1193:0:0. The default is 0:0:30. You can also set the value to 0, which means the connection never times out. A TCP connection for which a three-way handshake is not complete is an embryonic connection.
half-closed *hh* **:** *mm* **:** *ss*	Sets the idle timeout period until a half-closed connection is closed, between 0:5:0 (for 9.1(1) and earlier) or 0:0:30 (for 9.1(2) and later) and 1193:0:0. The default is 0:10:0. You can also set the value to 0, which means the connection never times out. Half-closed connections are not affected by DCD. Also, the ASA does not send a reset when taking down half-closed connections.
idle *hh* **:** *mm* **:** *ss*	Sets the idle timeout period after which an established connection of any protocol closes. The valid range is from 0:0:1 to 1193:0:0.

reset	For TCP traffic only, sends a TCP RST packet to both end systems after idle connections are removed.

Command Default

Unless you change the default globally using the timeout command, the defaults are:

- The default **embryonic** timeout is 30 seconds.
- The default **half-closed** idle timeout is 10 minutes.
- The default **dcd** *max_retries* value is 5.
- The default **dcd** *retry_interval* value is 15 seconds.
- The default **idle** timeout is 1 hour.
- The default **udp** idle timeout is 2 minutes.
- The default **icmp** idle timeout is 2 seconds.
- The default **esp** and **ha** idle timeout is 30 seconds.
- For all other protocols, the default idle timeout is 2 minutes.
- To never time out, enter 0:0:0.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Support for DCD was added.
8.2(2)	The **tcp** keyword was deprecated in favor of the **idle** keyword, which controls the idle timeout for all protocols.
9.1(2)	The minimum **half-closed** value was lowered to 30 seconds (0:0:30).
9.13(1)	The DCD configuration is now supported in a cluster.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command. Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection timeout** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the CLI configuration guide.

The **show service-policy** command to includes counters to show the amount of activity from DCD.

Examples

The following example sets the connection timeouts for all traffic:

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# policy-map CONNS
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
ciscoasa(config-pmap-c)# service-policy CONNS interface outside
```

You can enter **set connection** commands with multiple parameters, or you can enter each parameter as a separate command. The ASA combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
ciscoasa(config-pmap-c)# set connection timeout idle 2:0:0
ciscoasa(config-pmap-c)# set connection timeout embryonic 0:40:0
```

Then the output of the **show running-config policy-map** command would display the result of the two commands in the following single, combined command:

```
set connection timeout idle 2:0:0 embryonic 0:40:0
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configure connection values.
show running-config policy-map	Display all current policy-map configurations.
show service-policy	Displays counters for DCD and other service activity.

set default interface

The set interface command when used with default option will imply that the first attempt to route the matching traffic has to be done through normal route-lookup by looking up for an explicit route. Only when normal route-lookup fails, PBR will forward the traffic using the interface specified. Since both 'default' triggered lookup and the interface option triggered lookup depend on the presence of an explicit route to destination. Always 'default' lookup will succeed. When 'default' lookup fails, it means there is no explicit route to destination. So, interface action cannot be applied. When "set default interface" is configured, only 'Null0' can be configured as interface. When this option is configured, if normal route lookup does not yield an explicit route (non-default route) to the destination, traffic will be dropped.

set default interface Null0
no set default interface Null0

Syntax Description

interface	Interface to which packets are forwarded.

Command Default

There is no default for this command and Null0 interface has to be specified as set action.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Use this command to provide certain users a different default route. If the ASA has no explicit route for the destination, then it routes the packet to this interface. The first interface specified with the set default interface command that is up is used. The optionally specified interfaces are tried in turn.

Use the ip policy route-map interface configuration command, the route-map global configuration command, and the match and set route-map configuration commands to define the conditions for policy routing packets. The ip policy route-map command identifies a route map by name. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which policy routing occurs. The set commands specify the set actions—the particular routing actions to perform if the criteria enforced by the match commands are met.

In PBR for IPv6, use the ipv6 policy route-map or ipv6 local policy route-map command with match and set route map configuration commands to define conditions for policy routing packets.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. set ip next-hop

2. set interface

3. set ip default next-hop

4. set default interface

Examples

```
(config)# route-map testmap
(config-route-map)# set default interface Null0
(config)# show run route-map
!
route-map testmap permit 10
  set default interface Null0
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                default interface Null0
```

set dscp

The set dscp command is used to set the QoS bits in the matching IP packets.

set ip dscp { **0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef** }
no set ip dscp
set ip dscp { **0-63 | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | default | ef** }
no set ip dscp

Syntax Description

0-63	numeric range of dscp value.
af	assured forwarding class
ef	expedited forwarding
default	
cs	

Command Default

The DSCP value in the ToS byte is not set.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Once the DSCP bit is set, other quality of service (QoS) features can then operate on the bit settings.

DSCP and Precedence Values Are Mutually Exclusive

The set dscp command cannot be used with the set precedence command to mark the same packet. The two values, DSCP and precedence, are mutually exclusive. A packet can have one value or the other, but not both.

Precedence Value and Queuing

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data then is queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Use of the “from-field” Packet-marking Category

If you are using this command as part of the Enhanced Packet Marking feature, it can specify the “from-field” packet-marking category to be used for mapping and setting the DSCP value. The “from-field” packet-marking categories are as follows:

- Class of service (CoS)
- QoS group

If you specify a “from-field” category but do not specify the table keyword and the applicable table-map-name argument, the default action will be to copy the value associated with the “from-field” category as the DSCP value. For instance, if you configure the set dscp cos command, the CoS value will be copied and used as the DSCP value.

Note The CoS field is a three-bit field, and the DSCP field is a six-bit field. If you configure the set dscp cos command, only the three bits of the CoS field will be used.

If you configure the set dscp qos-group command, the QoS group value will be copied and used as the DSCP value.

The valid value range for the DSCP is a number from 0 to 63. The valid value range for the QoS group is a number from 0 to 99. Therefore, when configuring the set dscp qos-group command, note the following points:

- If a QoS group value falls within both value ranges (for example, 44), the packet-marking value will be copied and the packets will be marked.
- If QoS group value exceeds the DSCP range (for example, 77), the packet-marking value will not be copied and the packet will not be marked. No action is taken.

Set DSCP Values in IPv6 Environments

When this command is used in IPv6 environments, the default match occurs on both IP and IPv6 packets. However, the actual packets set by this function are only those that meet the match criteria of the class map containing this function.

Set DSCP Values for IPv6 Packets Only

To set DSCP values for IPv6 values only, you must also use the match protocol ipv6 command. Without that command, the precedence match defaults to match both IPv4 and IPv6 packets.

Set DSCP Values for IPv4 Packets Only

To set DSCP values for IPv4 values only, you must use the appropriate match ip command. Without this command, the class map may match both IPv6 and IPv4 packets, depending on the other match criteria, and the DSCP values may act upon both types of packets.

Examples

```
(config)# route-map testmapv4
(config-route-map)# set ip dscp af22
(config)# show run route-map
!
route-map testmapv4 permit 10
```

```
  set ip dscp af22
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip dscp af22
(config)# route-map testmapv6
(config-route-map)# set ipv6 dscp cs6
(config)# show run route-map
!
route-map testmapv6 permit 10
  set ipv6 dscp cs6
!
(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                ipv6 dscp cs6
```

set ikev1 transform-set

To specify the IPsec IKEv1 proposal for the IPsec profile, use the set ikev1 transform-set command in the IPsec profile configuration mode. Use the no form of this command to remove the IPsec IKEv1 proposal.

set ikev1 transform-set *transform-set name*
no set ikev1 transform-set *transform-set name*

Syntax Description

transform-set name	Specifies the name of the IPsec IKEv1 proposal.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec profile configuration	• Yes	• No	• Yes	• No	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following example specifies the IKEv1 proposal for the IPsec profile:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set ikev1 transform-set
```

Related Commands

Command	Description
crypto ipsec profile	Creates a new IPsec profile.
responder-only	Sets the VTI tunnel interface to responder only mode.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.
set security-association lifetime	Specifies the duration of security association in the IPsec profile configuration. This is specified in kilobytes or seconds, or both.
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

set interface

The set interface command is used to configure the interface through which the matching traffic has to be forwarded. It is allowed to configure multiple interfaces in which case they are evaluated in the specified order until a valid up and running interface to forward the packets is found. When the interface name is specified as 'Null0', all traffic matching the route-map will be dropped.

set interface [*...interface*]
no set interface [*...interface*]

Syntax Description

interface	Interface to which packets are forwarded.

Command Default

No command defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Use the ip policy route-map interface configuration command, the route-map global configuration command, and the match and set route-map configuration commands to define the conditions for policy-routing packets. The ip policy route-map command identifies a route map by name. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which policy routing occurs. The set commands specify the set actions—the particular routing actions to perform if the criteria enforced by the match commands are met.

In PBR for IPv6, use the ipv6 policy route-map or ipv6 local policy route-map command with match and set route-map configuration commands to define conditions for policy-routing packets.

If the first interface specified with the set interface command is down, the optionally specified interfaces are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. set ip next-hop
2. set interface
3. set ip default next-hop
4. set default interface

A useful next hop implies an interface. As soon as a next hop and an interface are found, the packet is routed.

Examples

```
ciscoasa(config)# route-map testmap
ciscoasa(config-route-map)# set interface outside
ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  set interface outside
!
ciscoasa(config)# show route-map testmap
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                interface outside
```

set ip df

The set ip df command is used to set the df (do-not-fragment) bit in the matching IP packets..

set ip df [**0** | **1**]
no set ip df

Syntax Description

0 Sets the df bit to 0 (clears the df bit), allows packets fragmentation.	
1 Sets the DF bit to 1 which prohibits packet fragmentation.	

Command Default

There is no default for this command and either 0 or 1 has to be specified as DF bit, in the set action.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Using Path MTU Discovery (PMTUD) you can determine an MTU value for IP packets that avoids fragmentation. If ICMP messages are blocked by a router, the path MTU is broken and packets with the DF bit set are discarded. Use the set ip df command to clear the DF bit and allow the packet to be fragmented and sent. Fragmentation can slow the speed of packet forwarding on the network but access lists can be used to limit the number of packets on which the DF bit will be cleared.

Note Some IP transmitters (notably some versions of Linux) may set the identification field in the IP header (IPid) to zero when the DF bit is set. If the router should clear the DF bit on such a packet and if that packet should subsequently be fragmented, then the IP receiver will probably be unable to correctly reassemble the original IP packet.

Examples

```
(config)# route-map testmap
(config-route-map)# set ip df 1
(config)# show run route-map
!
route-map testmap permit 10
  set ip df 1
!
(config)# show route-map testmap
```

```
route-map testmap, permit, sequence 10
   Match clauses:
   Set clauses:
                ip df 1
```

set ip default next-hop

The set ip next-hop command when used with the default option implies that the first attempt to route the matching traffic has to be done through normal route-lookup by looking for an explicit route. Only when normal route-lookup fails, Policy Based Routing (PBR) will forward the traffic using the specified next-hop ip address.

set ip default next-hop ip-address [*...ip-address*]
no set ip default next-hop ip-address [*...ip-address*]
set default ipv6next-hop ip-address [*...ip-address*]
no set default ipv6next-hop ip-address [*...ip-address*]

Syntax Description

ip-address	IP address of the next hop to which packets are output. It need not be an adjacent router.
ipv6-address	IPv6 address of the next hop to which packets are output. It need not be an adjacent router.

Command Default

This command is disabled by default and at least one next-hop ip address has to be specified for the set action.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Use this command to provide certain users a different default route. If the software has no explicit route for the destination in the packet, then it routes the packet to this next hop. The first next hop specified with the set ip default next-hop command needs to be adjacent to the router. The optional specified IP addresses are tried in turn.

Use the ip policy route-map interface configuration command, the route-map global configuration command, and the match and set route-map configuration commands to define the conditions for policy routing packets. The ip policy route-map command identifies a route map by name. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria--the conditions under which policy routing occurs. The set commands specify the set actions--the particular routing actions to perform if the criteria enforced by the match commands are met.

If the first next hop specified with the set next-hop command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. set next-hop

2. set interface
3. set default next-hop
4. set default interface

Note The set ip next-hop and set ip default next-hop are similar commands but have a different order of operations. Configuring the set ip next-hop command causes the system to use policy routing first and then use the routing table. Configuring the set ip default next-hop command causes the system to use the routing table first and then policy route the specified next hop.

Examples

```
(config)# route-map testmapv4
(config-route-map)# set ip default next-hop 1.1.1.1
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip default next-hop 1.1.1.1
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
Match clauses:
Set clauses:
ip default next-hop 1.1.1.1
(config)# route-map testmapv6
(config-route-map)# set ipv6 default next-hop 2001::1
(config)# show run route-map
!
route-map testmapv6 permit 10
  set ipv6 default next-hop 2001::1
!
(config)# show route-map testmapv6
route-map testmapv6, permit, sequence 10
Match clauses:
Set clauses:
ipv6 default next-hop 2001::1
```

set ip next-hop

To indicate where to output packets that pass a match clause of a route map for policy routing, use the set ip next-hop command in route-map configuration mode. To delete an entry, use the no form of this command.

set ip next-hop *ip-address* [*ip-address*] [**peer-address**]
no set ip next-hop *ip-address* [*ip-address*] [**peer-address**]
set ipv6 next-hop

Syntax Description

ip-address	IP address of the next hop to which packets are output. It need not be an adjacent router.
peer-address	(Optional) Sets the next hop to be the BGP peering address.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the ip-address argument.

Use the ip policy route-map interface configuration command, the route-map global configuration command, and the match and set route-map configuration commands to define the conditions for policy routing packets. The ip policy route-map command identifies a route map by name. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which policy routing occurs. The set commands specify the set actions—the particular routing actions to perform if the criteria enforced by the match commands are met.

If the first next hop specified with the set next-hop command is down, the optionally specified IP addresses are tried in turn.

When the set next-hop command is used with the peer-address keyword in an inbound route map of a BGP peer, the next hop of the received matching routes will be set to be the neighbor peering address, overriding any third-party next hops. So the same route map can be applied to multiple BGP peers to override third-party next hops.

When the set next-hop command is used with the peer-address keyword in an outbound route map of a BGP peer, the next hop of the advertised matching routes will be set to be the peering address of the local router, thus disabling the next hop calculation. The set next-hop command has finer granularity than the (per-neighbor)

neighbor next-hop-self command, because you can set the next hop for some routes, but not others. The neighbor next-hop-self command sets the next hop for all routes sent to that neighbor.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. set next-hop

2. set interface

3. set default next-hop

4. set default interface

Note To avoid a common configuration error for reflected routes, do not use the set next-hop command in a route map to be applied to BGP route reflector clients.

Examples

In the following example, three routers are on the same LAN (with IP addresses 10.1.1.1, 10.1.1.2, and 10.1.1.3). Each is in a different autonomous system. The set ip next-hop peer-address command specifies that traffic from the router (10.1.1.3) in remote autonomous system 300 for the router (10.1.1.1) in remote autonomous system 100 that matches the route map is passed through the router bgp 200, rather than sent directly to the router (10.1.1.1) in autonomous system 100 over their mutual connection to the LAN.

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.1.1.3 remote-as 300
ciscoasa(config-router-af)# neighbor 10.1.1.3 route-map set-peer-address out
ciscoasa(config-router-af)# neighbor 10.1.1.1 remote-as 100
ciscoasa(config-route-af)# route-map set-peer-address permit 10
ciscoasa(config-route-map)# set ip next-hop peer-address
```

set ip next-hop recursive

Both set ip next-hop and set ip default next-hop require that the next-hop be found on a directly connected subnet. With set ip next-hop recursive, the next-hop address does not need to be directly connected. Instead a recursive lookup is performed on the next-hop address, and matching traffic is forwarded to the next-hop used by that route entry according to the routing path in use on the router.

Recursive next-hop lookup is not applicable for IPv6 or when default keyword is specified.

set ip next-hop recursive [*ipv4-address*]
no set ip next-hop recursive [*ipv4-address*]

Syntax Description

ipv4-address	IP address of the next hop to which packets are output. It need not be an adjacent router.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

Use the ip policy route-map interface configuration command, the route-map global configuration command, and the match and set route-map configuration commands to define the conditions for policy routing packets. The ip policy route-map command identifies a route map by name. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which policy routing occurs. The set commands specify the set actions—the particular routing actions to perform if the criteria enforced by the match commands are met.

If the interface associated with the first next hop specified with the set ip next-hop command is down, the optionally specified IP addresses are tried in turn.

The set clauses can be used in conjunction with one another. They are evaluated in the following order:

1. set ip next-hop

2. set interface

3. set ip default next-hop

4. set default interface

Note The set ip next-hop and set ip default next-hop are similar commands but have a different order of operations. Configuring the set ip next-hop command causes the system to use policy routing first and then use the routing table. Configuring the set ip default next-hop command causes the system to use the routing table first and then policy route the specified next hop.

Examples

```
(config)# route-map testmapv4
(config-route-map)# set ip next-hop recursive 1.1.1.1
(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip next-hop recursive 1.1.1.1
!
(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip next-hop recursive 1.1.1.1
```

set ip next-hop verify-availability

The set ip next-hop verify-availability can be configured with an SLA monitor tracking object to verify the reachability of the next-hop. To verify the availability of multiple next-hops, multiple set ip next-hop verify-availability commands can be configured with different sequence numbers and different tracking objects.

set ip next-hop verify-availability [*sequence number*] **track** [*tracked-object-number*]
no set ip next-hop verify-availability [*sequence number*] **track** [*tracked-object-number*]

Syntax Description

sequence-number	Sequence of next hops. The acceptable range is from 1-65535.
track	The tracking method is track.
tracked-object-number	Object number that the tracking subsystem is tracking. The acceptable range is from 1 to 500.

Command Default

No command defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

The set ip next-hop verify-availability command can be used in the following two ways:

- With policy-based routing (PBR) to verify next hop reachability using Cisco Discovery Protocol (CDP).
- With optional arguments to support object tracking using Internet Control Message Protocol (ICMP) ping or an HTTP GET request to verify if a remote device is reachable.

Using CDP Verification

This command is used to verify that the next hop is reachable before the router tries to policy route to it. This command has the following characteristics:

- It causes some performance degradation.
- CDP must be configured on the interface.
- The next hop must be a Cisco device with CDP enabled.

- It is supported in process switching and Cisco Express Forwarding (CEF) policy routing, but is not available in distributed CEF (dCEF) because of the dependency of the CDP neighbor database.

If the router is policy routing packets to the next hop and the next hop is down, the router will try unsuccessfully to use Address Resolution Protocol (ARP) for the next hop (which is down). This behavior will continue indefinitely. To prevent this situation from occurring, use the set ip next-hop verify-availability command to configure the router to verify that the next hop of the route map is a CDP neighbor before routing to that next hop.

This command is optional because some media or encapsulations do not support CDP, or it may not be a Cisco device that is sending traffic to the router.

If this command is set and the next hop is not a CDP neighbor, then the router looks to the subsequent next hop, if there is one. If there is no next hop, the packets are not policy routed.

If this command is not set, the packets are either successfully policy routed or remain forever unrouted.

If you want to selectively verify availability of only some next hops, you can configure different route map entries (under the same route map name) with different criteria (using access list matching or packet size matching), and then use the set ip next-hop verify-availability command selectively.

Using Object Tracking

With optional arguments to support object tracking, this command allows PBR to make decisions based on the following criteria:

- ICMP ping reachability to a remote device.
- Application running on a remote device (for example, the device responds to an HTTP GET request).
- A route exists in the Routing Information Base (RIB) (for example, policy route only if 10.2.2.0/24 is in the RIB).
- Interface state (for example, packets received on E0 should be policy routed out E1 only if E2 is down).

Object tracking functions in the following manner. PBR will inform the tracking process that it is interested in tracking a certain object. The tracking process will in turn notify PBR when the state of the object changes. This notification is done via registries and is event driven.

The tracking subsystem is responsible for tracking the state of an object. The object can be an IP address that is periodically being pinged by the tracking process. The state of the object (up or down) is stored in a track report data structure. The tracking process will create the tracking object report. Then the exec process that is configuring the route map can query the tracking process to determine if a given object exists. If the object exists, the tracking subsystem can start tracking it and read the initial state of the object. If the object changes state, the tracking process will notify all the clients that are tracking this process that the state of the object has changed. So, the route map structure that PBR is using can be updated to reflect the current state of the object in the track report. This interprocess communication is done by means of registries and the shared track report.

Note If the CDP and object tracking commands are mixed, the tracked next hops will be tried first.

Examples

```
ciscoasa(config)# sla monitor 1
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 1.1.1.1 interface outside
ciscoasa(config)# sla monitor schedule 1 life forever start-time now
ciscoasa(config)# track 1 rtr 1 reachability
ciscoasa(config)#
ciscoasa(config)# route-map testmapv4
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.1 10 track 1
ciscoasa(config)# show run route-map
!
route-map testmapv4 permit 10
  set ip next-hop verify-availability 1.1.1.1 10 track 1
!
ciscoasa(config)# show route-map testmap
route-map testmapv4, permit, sequence 10
   Match clauses:
   Set clauses:
                ip next-hop verify-availability 1.1.1.1 10 track 1
```

set local-preference

To specify a preference value for the autonomous system path, use the **set local-preference** command in route-map configuration mode. To delete an entry, use the **no**form of this command.

set local-preference *number-value*
no set local-preference *number-value*

Syntax Description

number-value	Preference value. An integer from 0 to 4294967295.

Command Default

Preference value is 100.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The preference is sent only to all routers in the local autonomous system.

Use the **route-map** global configuration command, and the **match** and **set** route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a list of **match** and **set** commands associated with it. The **match** commands specify the *match criteria* --the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the *set actions*--the particular redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **set** route-map configuration commands specify the redistribution *set actions* to be performed when all the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

You can change the default preference value with the bgp default local-preference command.

Examples

The following example sets the local preference to 100 for all routes that are included in access list 1:

```
ciscoasa(config-route-map)# route-map map-preference
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

set metric

To set the metric value of a route for OSPF and other dynamic routing protocols in a route map, use the set metric command in route-map configuration mode. To return to the default metric value for OSPF and other dynamic routing protocols, use the **no** form of this command.

set metric *metric-value* | [*bandwidth delay reliability loading mtu*]
no set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

Syntax Description

bandwidth	EIGRP bandwidth of a route, in kbps. Valid values range from 0 to 4294967295.
delay	EIGRP route delay, in tens of microseconds. Valid values range from 0 to 4294967295.
loading	Effective EIGRP bandwidth of a route expressed as a number from 0 to 255. The value 255 means 100 percent loading.
metric-value	Metric value of a route for OSPF and other dynamic routing protocols (except for EIGRP), expressed as a number. Valid values range from 0 to 4294967295.
mtu	Minimum MTU size of a route for EIGRP, in bytes. Valid values range from 0 to 4294967295.
reliability	Likelihood of successful packet transmission for EIGRP expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(5)	The *bandwidth* , *delay*, *reliability*, *loading*, and *mtu* arguments to support EIGRP in a route map were added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **no** set metric command allows you to return to the default metric value for OSPF and other dynamic routing protocols. In this context, the *metric-value* argument is an integer from 0 to 4294967295.

Examples

The following example shows how to configure a route map for OSPF routing:

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
```

The following example shows how to set the metric value for EIGRP in a route map:

```
ciscoasa(config)# access-list route-out line 1 standard permit 10.1.1.0 255.255.255.0
ciscoasa(config)# route-map rmap permit 10
ciscoasa(config-route-map)# set metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show route-map rmap
route-map rmap, permit, sequence 10
  Match clauses:
    ip address (access-lists): route-out
  Set clauses:
    metric 10000 60 100 1 1500
ciscoasa(config-route-map)# show running-config route-map
route-map rmap permit 10
 match ip address route-out
 set metric 10000 60 100 1 1500
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out of one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

set metric-type

To specify the type of OSPF metric routes, use the set metric-type command in route-map configuration mode. To return to the default setting, use the **no** form of this command.

set metric-type { **type-1** | **type-2** }
no set metric-type

Syntax Description

type-1	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
type-2	Specifies the type of OSPF metric routes that are external to a specified autonomous system.

Command Default

The default is type-2.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows how to configure a route map for OSPF routing:

```
ciscoasa(config)# route-map maptag1 permit 8
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# match metric 5
ciscoasa(config-route-map)# set metric-type type-2
ciscoasa(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
ciscoasa(config-route-map)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,

Command	Description
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

set metric-type internal

To set the Multi Exit Discriminator (MED) value on prefixes advertised to external BGP (eBGP) neighbors to match the Interior Gateway Protocol (IGP) metric of the next hop, use the set metric-type internal command in route-map configuration mode. To return to the default, use the no form of this command.

set metric-type internal
no set metric-type internal

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	We added this command.

Usage Guidelines

This command will cause BGP to advertise a MED value that corresponds to the IGP metric associated with the next hop of the route. This command applies to generated, internal BGP (iBGP)-, and eBGP-derived routes.

If this command is used, multiple BGP speakers in a common autonomous system can advertise different MED values for a particular prefix. Also, note that if the IGP metric changes, BGP will readvertise the route every 10 minutes.

Use the route-map global configuration command and the match and set route-map configuration commands to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of the route map are met. When all match criteria are met, all set actions are performed.

Note This command is not supported for redistributing routes into the Border Gateway Protocol (BGP).

Examples

In the following example, the MED value for all the advertised routes to neighbor 172.16.2.3 is set to the corresponding IGP metric of the next hop:

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 172.16.0.0
ciscoasa(config-router-af)# neighbor 172.16.2.3 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.2.3 route-map setMED out
ciscoasa(config-route-map)# route-map setMED permit 10
ciscoasa(config-route-map)# match as-path as-path-acl
ciscoasa(config-route-map)# set metric-type internal
ciscoasa(config-route-map)# ip as-path access-list as-path-acl permit .*
```

set origin

To set the BGP origin code, use the set origin command in route-map configuration mode. To delete an entry, use the no form of this command.

set origin { **igp | egp** *autonomous-system-number* | **incomplete** }
no set origin { **igp | egp** *autonomous-system-number* | **incomplete** }

Syntax Description

autonomous-system-number	Number of a remote autonomous system number. The range of values for this argument is any valid autonomous system number from 1 to 65535.
egp	Local External Gateway Protocol (EGP) system.
igp	Remote Interior Gateway Protocol (IGP) system.
incomplete	Unknown heritage.

Command Default

The origin of the route is based on the path information of the route in the main IP routing table.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You must have a match clause (even if it points to a "permit everything" list) if you want to set the origin of a route. Use this command to set a specific origin when a route is redistributed into BGP. When routes are redistributed, the origin is usually recorded as incomplete, identified with a ? in the BGP table.

Use the route-map global configuration command, and the match and set route-map configuration commands, to define the conditions for redistributing routes from one routing protocol into another. Each route-map command has a list of match and set commands associated with it. The match commands specify the match criteria—the conditions under which redistribution is allowed for the current route-map command. The set commands specify the set actions—the particular redistribution actions to perform if the criteria enforced by the match commands are met. The no route-map command deletes the route map.

The set route-map configuration commands specify the redistribution set actions to be performed when all of the match criteria of a route map are met. When all match criteria are met, all set actions are performed.

Examples

The following example sets the origin of routes that pass the route map to IGP:

```
ciscoasa(config-route-map)# route-map set_origin
ciscoasa(config-route-map)# match as-path 10
ciscoasa(config-route-map)# set origin igp
```

set pfs

To specify the PFS group for the IPsec profile, use the set pfs command in the IPsec profile configuration mode. Use the no form of this command to remove the PFS group.

set pfs *Diffie-Hellman group* [**group14**]
no set pfs *Diffie-Hellman group* [**group14**]

Syntax Description

Diffie-Hellman group	Specifies the name of the *Diffie-Hellman group (dh group)*.
group14	Specifies that IPsec should use the 2048-bit Diffie-Hellman prime modulus group when performing the new Diffie-Hellman exchange.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec profile configuration	• Yes	• No	• Yes	• No	—

Command History

Release	Modification
9.16(1)	Support was added for the group31 command option.
9.15(1)	Support was removed for the group2 and group5 command options.
9.13(1)	Added support for Group 14. The group2 and group5 command options was deprecated and will removed in the later release.
9.7(1)	We introduced this command.

Examples

The following example sets group14 as the pfs:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set pfs group14
```

Related Commands

Command	Description
crypto ipsec profile	Creates a new IPsec profile.
responder-only	Sets the VTI tunnel interface to responder only mode.

Command	Description
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set security-association lifetime	Specifies the duration of security association in the IPsec profile configuration. This is specified in kilobytes or seconds, or both.
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

set security-association lifetime

To specify the duration of security association in the IPsec profile configuration, use the **set security-association lifetime** command in the IPsec profile configuration mode. This is specified in kilobytes or seconds, or both. Use the **no** form of this command to remove the security association lifetime configuration.

set security-association lifetime { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }
no set security-association lifetime { **seconds** *number* | **kilobytes** { *number* | **unlimited** } }

Syntax Description

kilobytes { *number* | **unlimited** }	Specifies the volume of traffic (in kilobytes) that can pass between peers using a given security association before that security association expires. The range is 10 to 2147483647 kbytes. The global default is 4,608,000 kilobytes. This setting does not apply to remote access VPN connections. It applies to site-to-site VPN only.
seconds *number*	Specifies the number of seconds a security association will live before it expires. The range is 120 to 214783647 seconds. The global default is 28,800 seconds (eight hours). This setting applies to both remote access and site-to-site VPN.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec profile configuration	• Yes	• No	• Yes	• No	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

IPsec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the ASA requests new security associations during security association negotiation, it specifies its crypto map lifetime values in the request to the peer; it uses these values as the lifetime of the new security associations. When the ASA receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime values as the lifetime of the new security associations.

For site-to-site VPN connections, there are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after the first of these lifetimes is reached. For remote access VPN sessions, only the timed lifetime applies.

Note The ASA lets you change crypto map, dynamic map, and IPsec settings on-the-fly. If you do so, the ASA brings down only the connections affected by the change. If you change an existing access list associated with a crypto map, specifically by deleting an entry within the access list, the result is that only the associated connection is brought down. Connections based on other entries in the access list are not affected.

Examples

The following example sets the security association lifetime values:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set security-association lifetime seconds 120 kilobytes
10000
```

Related Commands

Command	Description
crypto ipsec profile	Creates a new IPsec profile.
responder-only	Sets the VTI tunnel interface to responder only mode.
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.
set trustpoint	Specifies a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection.

set trustpoint

To specify a trustpoint that defines the certificate to be used while initiating a VTI tunnel connection, use the set trustpoint command in the IPsec profile configuration mode. Use the no form of this command to remove the trustpoint configuration.

set trustpoint *name* **chain**
no set trustpoint *name* **chain**

Syntax Description

name	Specifies the name of the trustpoint.
chain	Enables the sending of certificate chain.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPsec profile configuration	• Yes	• No	• Yes	• No	—

Command History

Release	Modification
9.8(1)	We introduced this command.

Examples

The following example sets the security association lifetime values:

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# set trustpoint TPVTI chain
```

Related Commands

Command	Description
crypto ipsec profile	Creates a new IPsec profile.
responder-only	Sets the VTI tunnel interface to responder only mode.
set ikev1 transform-set	Specifies the IKEv1 transform set to be used in the IPsec profile configuration.
set pfs	Specifies the PFS group to be used in the IPsec profile configuration.

setup

To configure a minimal configuration for the ASA using interactive prompts, enter the **setup** command in global configuration mode.

setup

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	In routed mode for the ASA 5510 and higher, the interface configured is now the Management *slot /port* interface, and not the "inside" interface. For the ASA 5505, the interface configured is the VLAN 1 interface, not "inside".
9.0(1)	The default configuration prompt was changed, and Ctrl + Z to exit the setup process was enabled.

Usage Guidelines

The setup prompt automatically appears at boot time if there is no startup configuration in flash memory.

The **setup** command walks you through minimal configuration to establish ASDM connectivity. This command is designed for a unit that has either no configuration or a partial configuration. If your model supports a factory default configuration, we recommend using the factory default configuration instead of the **setup** command (to restore the default configuration, use the **configure factory-default** command).

The **setup** command requires an already-named interface called "management."

When you enter the **setup** command, you are asked for the information in XREF. If there is already a configuration for the listed parameter, it appears in brackets, so you can either accept it as the default or override it by entering a new value. The exact prompts available may differ per model. The system **setup** command includes a subset of these prompts.

Table 1: Setup Prompts

Prompt	Description
`Pre-configure Firewall now through interactive prompts [yes]?`	Enter **yes** or **no**. If you enter **yes**, the setup continues. If **no**, the setup stops and the global configuration prompt (ciscoasa(config)#) appears.
`Firewall Mode [Routed]:`	Enter **routed** or **transparent**.
`Enable password:`	Enter an enable password. (The password must have at least three characters.)
`Allow password recovery [yes]?`	Enter **yes** or **no**.
`Clock (UTC):`	You cannot enter anything in this field. The UTC time is used by default.
`Year:`	Enter the year using four digits, for example, 2005. The year range is 1993 to 2035.
`Month:`	Enter the month using the first three characters of its name, for example, **Sep** for September.
`Day:`	Enter the day of the month, from 1 to 31.
`Time:`	Enter the hour, minutes, and seconds in 24-hour time format, for example, enter **20:54:44** for 8:54 p.m and 44 seconds.
`Host name:`	Enter the hostname that you want to display in the command line prompt.
`Domain name:`	Enter the domain name of the network on which the ASA runs.
`IP address of host running Device Manager:`	Enter the IP address of the host that needs to access ASDM.
`Use this configuration and save to flash (yes)?`	Enter **yes** or **no**. If you enter **yes**, the inside interface is enabled and the requested configuration is written to the Flash partition. If you enter **no**, the setup prompt repeats, beginning with the first question: `Pre-configure Firewall now through interactive prompts [yes]?` Enter **Ctrl + Z** to exit the setup or **yes** to repeat the prompt.

Examples

The following example shows how to complete the **setup** command:

```
ciscoasa(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
```

```
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1
The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1
Use this configuration and write to flash? yes
```

Related Commands

Command	Description
configure factory-default	Restores the default configuration.

set weight

To specify the BGP weight for the routing table, use the set weight command in route-map configuration mode. To delete an entry, use the no form of this command.

set weight *number*
no set weight *number*

Syntax Description

number	Weight value. It can be an integer ranging from 0 to 65535.

Command Default

The weight is not changed by the specified route map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Route-map configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

The implemented weight is based on the first matched autonomous system path. Weights indicated when an autonomous system path is matched override the weights assigned by global neighbor commands. In other words, the weights assigned with the set weight route-map configuration command override the weights assigned using the neighbor weight command.

Examples

The following example sets the BGP weight for the routes matching the autonomous system path access list to 200:

```
ciscoasa(config-route-map)# route-map set-weight
ciscoasa(config-route-map)# match as-path as_path_acl
iscoasa(config-route-map)# set weight 200
```

sfr

To redirect traffic to the ASA FirePOWER module, use the **sfr** command in class configuration mode. To remove the redirect, use the **no** form of this command.

sfr { **fail-close | fail-open** } [**monitor-only**]
no sfr { **fail-close | fail-open** } [**monitor-only**]

Syntax Description

fail-close	Sets the ASA to block the traffic if the module is unavailable.
fail-open	Sets the ASA to allow the traffic through, applying ASA policies only, if the module is unavailable.
monitor-only	Sends a read-only copy of traffic to the module, i.e. passive mode. If you do not include the keyword, the traffic is sent in inline mode.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You can access the class configuration mode by first entering the policy-map command.

Before or after you configure the **sfr** command on the ASA, configure the security policy on the module using Secure Firewall Management Center (formerly Firepower Management Center).

To configure the **sfr** command, you must first configure the **class-map** command, **policy-map** command, and the **class** command.

Traffic Flow

The ASA FirePOWER module runs a separate application from the ASA. It is, however, integrated into the ASA traffic flow. When you apply the **sfr** command for a class of traffic on the ASA, traffic flows through the ASA and the module in the following way:

1. Traffic enters the ASA.

2. Incoming VPN traffic is decrypted.

3. Firewall policies are applied.

4. Traffic is sent to the ASA FirePOWER module over the backplane.

5. The module applies its security policy to the traffic and takes appropriate actions.

6. In inline mode, valid traffic is sent back to the ASA over the backplane; the ASA FirePOWER module might block some traffic according to its security policy, and that traffic is not passed on. In passive mode, no traffic is returned, and the module cannot block traffic.

7. Outgoing VPN traffic is encrypted.

8. Traffic exits the ASA.

Compatibility with ASA Features

The ASA includes many advanced application inspection features, including HTTP inspection. However, the ASA FirePOWER module provides more advanced HTTP inspection than the ASA provides, as well as additional features for other applications, including monitoring and controlling application usage.

To take full advantage of the ASA FirePOWER module features, see the following guidelines for traffic that you send to the ASA FirePOWER module:

Do not configure ASA inspection on HTTP traffic.

- Do not configure Cloud Web Security (ScanSafe) inspection. If you configure both ASA FirePOWER inspection and Cloud Web Security inspection for the same traffic, the ASA only performs ASA FirePOWER inspection.
- Other application inspections on the ASA are compatible with the ASA FirePOWER module, including the default inspections.
- Do not enable the Mobile User Security (MUS) server; it is not compatible with the ASA FirePOWER module.
- If you enable failover, when the ASA fails over, any existing ASA FirePOWER flows are transferred to the new ASA. The ASA FirePOWER module in the new ASA begins inspecting the traffic from that point forward; old inspection states are not transferred.

Monitor-Only Mode

The traffic flow in monitor-only mode is the same as it is for inline mode. The only difference is that the ASA FirePOWER module does not pass traffic back to the ASA. Instead, the module applies the security policy to the traffic and lets you know what it would have done if it were operating in inline mode, e.g. traffic might be marked “would have dropped” in events. You can use this information for traffic analysis and to help you decide if inline mode is desirable.

Note You cannot configure both monitor-only mode and normal inline mode at the same time on the ASA. Only one type of security policy is allowed. In multiple context mode, you cannot configure monitor-only mode for some contexts, and regular inline mode for others.

Examples

The following example diverts all HTTP traffic to the ASA FirePOWER module, and blocks all HTTP traffic if the module fails for any reason:

```
ciscoasa(config)# access-list ASASFR permit tcp any any eq port 80
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list ASASFR
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-close
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the ASA FirePOWER module, and allows all traffic through if the module fails for any reason.

```
ciscoasa(config)# access-list my-sfr-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-sfr-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-sfr-class
ciscoasa(config-cmap)# match access-list my-sfr-acl
ciscoasa(config)# class-map my-sfr-class2
ciscoasa(config-cmap)# match access-list my-sfr-acl2
ciscoasa(config-cmap)# policy-map my-sfr-policy
ciscoasa(config-pmap)# class my-sfr-class
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap)# class my-sfr-class2
ciscoasa(config-pmap-c)# sfr fail-open
ciscoasa(config-pmap-c)# service-policy my-sfr-policy interface outside
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
cxsc	Redirects traffic to the ASA CX module.
hw-module module reload	Reloads the module.
hw-module module reset	Performs a reset and then reloads the module.
hw-module module shutdown	Shuts down the module.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show asp table classify domain sfr	Shows the NP rules created to send traffic to the ASA FirePOWER module.
show module	Shows the module status.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Shows service policy statistics.
sw-module module sfr reload	Reloads the software module.
sw-module module sfr reset	Resets the software module.
sw-module module sfr recover	Installs the software module boot image.
sw-module module sfr shutdown	Shuts down the software module.

shape

To enable QoS traffic shaping, use the **shape** command in class configuration mode. If you have a device that transmits packets at a high speed, such as a ASA with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the ASA to transmit packets at a fixed slower rate, called *traffic shaping* . To remove this configuration, use the **no** form of this command.

Note Traffic shaping is only supported on the ASA 5505, 5510, 5520, 5540, and 5550. Multi-core models (such as the ASA 5500-X) do not support shaping.

shape average *rate* [*burst_size*]
no shape average *rate* [*burst_size*]

Syntax Description

average *rate*	Sets the average rate of traffic in bits per second over a given fixed time period, between 64000 and 154400000. Specify a value that is a multiple of 8000. See the "Usage Guidelines" section for more information about how the time period is calculated.
burst_size	Sets the average burst size in bits that can be transmitted over a given fixed time period, between 2048 and 154400000. Specify a value that is a multiple of 128. If you do not specify the *burst_size* , the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Command Default

If you do not specify the *burst_size* , the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Class configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.

Usage Guidelines

To enable traffic shaping, use the Modular Policy Framework:

1. **policy-map** —Identify the actions associated with the **class-default** class map.

a. **class class-default** —Identify the **class-default** class map on which you want to perform actions.

b. **shape** —Apply traffic shaping to the class map.

c. (Optional) **service-policy** —Call a different policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.

2. **service-policy** —Assigns the policy map to an interface or globally.

Traffic Shaping Overview

Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

- Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic.
- Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPsec header and L2 header.
- The shaped traffic includes both through-the-box and from-the-box traffic.
- The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the burst size value. See the CLI configuration guide for more information about the token bucket.
- When bursty traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queuing, see the **priority** command):
- The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200-milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.
- When the queue limit is reached, packets are tail-dropped.
- Certain critical keep-alive packets such as OSPF Hello packets are never dropped.
- The time interval is derived by *time_interval* = *burst_size* / *average_rate* . The larger the time interval is, the burstier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

Average Rate = 1000000

Burst Size = 1000000

In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay-sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

How QoS Fea tures Interact

You can configure each of the QoS features alone if desired for the ASA. Often, though, you configure multiple QoS features on the ASA so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).

You cannot configure priority queuing and policing for the same set of traffic.

- Traffic shaping (for all traffic on an interface) + Hierarchical priority queuing (for a subset of traffic).

You cannot configure traffic shaping and standard priority queuing for the same interface; only hierarchical priority queuing is allowed. For example, if you configure standard priority queuing for the global policy, and then configure traffic shaping for a specific interface, the feature you configured last is rejected because the global policy overlaps the interface policy.

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the ASA does not restrict you from configuring this.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
ciscoasa
(config)#
class-map TG1-voice
ciscoasa
(config-cmap)#
match tunnel-group tunnel-grp1
ciscoasa
(config-cmap)#
match dscp ef
ciscoasa(config)# policy-map priority-sub-policy
ciscoasa(config-pmap)# class
            TG1-voice
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# policy-map shape_policy
ciscoasa(config-pmap)# class
            class-default
ciscoasa(config-pmap-c)# shape
ciscoasa(config-pmap-c)# service-policy priority-sub-policy
ciscoasa
(config-pmap-c)#
service-policy shape_policy
 interface outside
```

Related Commands

Command	Description
class	Identifies the class map on which you want to perform actions in a policy map.
police	Enables QoS policing.
policy-map	Identifies actions to apply to traffic in a service policy.
priority	Enables QoS priority queuing.
service-policy (class)	Applies a hierarchical policy map.
service-policy (global)	Applies a service policy to interface(s).
show service-policy	Shows QoS statistics.

share-ratio

To configure the port ratio, which determines how many ports are in the port pool in the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **share-ratio** command in MAP domain basic mapping rule configuration mode. Use the **no** form of this command to remove the ratio.

share-ratio*number*
no share-ratio *number*

Syntax Description

number	The number of ports that should be in the pool. The number must be a power of 2, from 1-65536, such as 1, 2, 4, 8, and so forth.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain basic mapping rule configuration mode.	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The **start-port** and **share-ratio** commands in the basic mapping rule determine the starting port and number of ports in the pool used to translate addresses within a MAP domain.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0

ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64

ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

show aa – show asr

show aaa kerberos

To display Kerberos service information, use the **show aaa kerberos** command in privileged EXEC mode.

show aaa kerberos [**username** *user*] | **keytab**]

Syntax Description

keytab	Displays information about the Kerberos keytab file.
username *user*	Displays tickets for the specified user.

Command Default

If you do not specify a keyword, tickets for all users are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Usage Guidelines

Use the **show aaa kerberos** command, without keywords, to view all the Kerberos tickets cached on the ASA. Add the **username** keyword to view the Kerberos tickets of a specific user. You must use the **keytab** keyword to see any information about the keytab file.

Examples

The following example shows the usage of the **show aaa kerberos** command:

```
ciscoasa
(config)# show aaa kerberos
Default Principal       Valid Starting     Expires     Service Principalkcduser@example.com
       06/29/10 17:33:00     06/30/10 17:33:00
asa$/mycompany.com@example.comkcduser@example.com       06/29/10 17:33:00     06/30/10
17:33:00    http/owa.mycompany.com@example.com
```

The following example shows how to display information about the Kerberos keytab file.

```
ciscoasa# show aaa kerberos keytab

Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
```

Related Commands

Command	Description
aaa kerberos import-keytab	Imports a Kerberos keytab file that you exported from the Kerberos Key Distribution Center (KDC).

Command	Description
clear aaa kerberos	Clears the cached Kerberos tickets.
show running-config aaa-server	Displays the AAA server configuration.

show aaa local user

To show the list of usernames that are currently locked, or to show details about the username, use the show **aaa local user** command in global configuration mode.

show aaa local user [**locked**]

Syntax Description

locked	(Optional) Shows the list of usernames that are currently locked.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	We added this command.
9.17(1)	Added **Expired** and **New-User** columns.

Usage Guidelines

If you omit the optional keyword **locked**, the ASA displays the failed-attempts and lockout status details for all AAA local users.

This command affects only the status of users that are locked out.

Users are unlocked after 10 minutes; however, the output of this command will still show a user as locked after 10+ minutes until they successfully log in again.

Examples

The following example shows use of the **show aaa** local user command to display the lockout status of all usernames:

This example shows the use of the **show aaa local user** command to display the number of failed authentication attempts and lockout status details for all AAA local users, after the limit has been set to 5:

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts     Expired     New-User     Locked      User
    -                   6      N            N           Y           cas
    -                   2      N            Y           N           sam
    -                   1      N            Y           N           dean
    -                   4      N            N           N           admin
```

```
ciscoasa(config)#
```

This example shows the use of the **show aaa local user** command with the **lockout** keyword to display the number of failed authentication attempts and lockout status details only for any locked-out AAA local users, after the limit has been set to 5:

```
ciscoasa(config)# aaa local authentication attempts max-fail 5
ciscoasa(config)# show aaa local user
Lock-time  Failed-attempts     Expired     New-User     Locked      User
    -                  6      N            N           Y           cas
ciscoasa(config)#
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Configures the maximum number of times a user can enter a wrong password before being locked out.
clear aaa local user fail-attempts	Resets the number of failed attempts to 0 without modifying the lockout status.
clear aaa local user lockout	Clears th e lockout status of the specified user or all users and sets their failed attempts counters to 0.

show aaa login-history

To view the login history, use the **show aaa login-history** command in privileged EXEC mode.

show aaa login-history [**user** *name*]

Syntax Description

user *name*	(Optional) Specifies the login history for a particular user.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Usage Guidelines

By default, the ASA saves the login history for usernames in the local database or from a AAA server when you enable local AAA authentication for one or more of the CLI management methods (SSH, Telnet, serial console). Use the **show aaa login-history** command to view the login history. See the **aaa authentication login-history** command to configure the history duration.

ASDM logins are not saved in the history.

The login history is only saved per unit; in failover and clustering environments, each unit maintains its own login history only.

Login history data is not maintained over reloads.

Examples

The following example shows the login history:

```
ciscoasa(config)# show aaa login-history
Login history for user:                            cisco
Logins in last   1 days:                           45
Last successful login:                          14:07:28 UTC Aug 21 2018 from 10.86.190.50
Failures since last login:                         0
Last failed login:                                 None
Privilege level:                                   14
Privilege level changed from 11 to 14 at:          14:07:30 UTC Aug 21 2018
```

Related Commands

Command	Description
aaa authentication login-history	Saves the local **username** login history.
password-history	Stores previous **username** passwords. This command is not user-configurable.

Command	Description
password-policy reuse-interval	Prohibits the reuse of a **username** password.
password-policy username-check	Prohibits a password that matches a **username** name.
show aaa login-history	Shows the local **username** login history.
username	Configures a local user.

show aaa sdi node-secrets

To display information about the SDI node secret files installed on the system, use the **show aaa sdi node-secrets** command in privileged EXEC mode.

show aaa sdi node-secrets

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Usage Guidelines

Use the **show aaa sdi node-secrets** command to view a list of the RSA SecurID servers that have node secret files installed on the system. The node secret files are exported from the RSA Authentication Manager, and uploaded to the system using the **aaa sdi import-node-secret** command. To remove a node secret file, use the **clear aaa sdi node-secret** command.

Examples

The following example shows the SecurID servers that have node secret files installed on the system.

```
ciscoasa
#
show aaa sdi node-secrets

Last update                    SecurID server
--------------------           --------------------
15:16:13 Jun 24 2020           rsaam.cisco.com
15:20:07 Jun 24 2020           10.11.12.13
ciscoasa
#
```

Related Commands

Command	Description
aaa sdi import-node-secret	Imports a node secret file that was exported from an RSA Authentication Manager.
clear aaa sdi node-secret	Removes a node secret file.

show aaa-server

To display AAA server statistics for AAA servers, use the **show aaa-server** command in privileged EXEC mode.

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

Syntax Description

LOCAL	(Optional) Shows statistics for the LOCAL user database.
groupname	(Optional) Shows statistics for servers in a group.
host *hostname*	(Optional) Shows statistics for a particular server in the group.
protocol *protocol*	(Optional) Shows statistics for servers of the following specified protocols: • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

Command Default

By default, all AAA server statistics display.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.1(1)	The http-form protocol was added.
8.0(2)	The server status shows if the status was changed manually using the **aaa-server active** command or **fail** command.

Examples

The following is sample output from the **show aaa-server** command:

```
ciscoasa(config)# show aaa-server group1 host 192.68.125.60
Server Group:  group1
Server Protocol: RADIUS
Server Address:  192.68.125.60
Server port:  1645
Server status: ACTIVE. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests        20
Average round trip time           4ms
Number of authentication requests 20
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         1
Number of accepts                 16
Number of rejects                 4
Number of challenges              5
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
```

The following table shows field descriptions for the **show aaa-server** command:

Field	Description
Server Group	The server group name specified by the **aaa-server** command.
Server Protocol	The server protocol for the server group specified by the **aaa-server** command.
Server Address	The IP address of the AAA server.
Server port	The communication port used by the ASA and the AAA server. You can specify the RADIUS authentication port using the **authentication-port** command. You can specify the RADIUS accounting port using the **accounting-port** command. For non-RADIUS servers, the port is set by the **server-port** command.

Field	Description

Server status	The status of the server. One of the following values appears:
	• ACTIVE—The ASA will communicate with this AAA server.
	• FAILED—The ASA cannot communicate with the AAA server. Servers that are put into this state remain there for some period of time, depending on the policy configured, and are then reactivated.
	If the status is followed by "(admin initiated)," then the server was manually failed or reactivated using the **aaa-server active** command or **fail** command.
	The date and time of the last transaction appear in the following form:
	`Last transaction ( {success | failure }) at time timezone date`
	If the ASA has never communicated with the server, the message shows as the following:
	`Last transaction at Unknown`

Number of pending requests	The number of requests that are still in progress.
Average round trip time	The average time that it takes to complete a transaction with the server.
Number of authentication requests	The number of authentication requests sent by the ASA. This value does not include retransmissions after a timeout.
Number of authorization requests	The number of authorization requests. This value refers to authorization requests due to command authorization, authorization for through-the-box traffic (for TACACS+ servers), or for WebVPN and IPsec authorization functionality enabled for a tunnel group. This value does not include retransmissions after a timeout.
Number of accounting requests	The number of accounting requests. This value does not include retransmissions after a timeout.
Number of retransmissions	The number of times a message was retransmitted after an internal timeout. This value applies only to Kerberos and RADIUS servers (UDP).
Number of accepts	The number of successful authentication requests.
Number of rejects	The number of rejected requests. This value includes error conditions as well as true credential rejections from the AAA server.

Field	Description
Number of challenges	The number of times the AAA server required additional information from the user after receiving the initial username and password information.
Number of malformed responses	N/A. Reserved for future use.
Number of bad authenticators	The number of times that one of the following occurs: • The “authenticator” string in the RADIUS packet is corrupted (rare). • The shared secret key on the ASA does not match the one on the RADIUS server. To fix this problem, enter the correct server key. This value only applies to RADIUS.
Number of timeouts	The number of times the ASA has detected that a AAA server is not responsive or otherwise misbehaving and has declared it offline.
Number of unrecognized responses	The number of times that the ASA received a response from the AAA server that it could not recognize or support. For example, the RADIUS packet code from the server was an unknown type, something other than the known “access-accept,” “access-reject,” “access-challenge,” or “accounting-response” types. Typically, this means that the RADIUS response packet from the server was corrupted, which is rare.

Related Commands

Command	Description
show running-config aaa-server	Displays statistics for all servers in the indicated server group or for a particular server.
clear aaa-server statistics	Clears the AAA server statistics.

show access-list

To display the hit counters and a timestamp value for an access list, use the **show access-list** command in privileged EXEC mode.

show access-list [*id* [*ip_address* | **brief** | **numeric**] | **element-count**]

Syntax Description

brief	(Optional) Displays the access list identifiers, the hit count, and the timestamp of the last rule hit, all in hexadecimal format.
id	(Optional) Shows counters for the ID of an existing access list.
ip_address	(Optional) Shows counters for the source IP address or hostname in the specified access list.
numeric	(Optional.) If you specify an ACL name, displays ports as numbers instead of names. For example, 80 instead of www.
element-count	(Optional.) Displays the total number of access control entries in all access lists defined on the system.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	Support for the **brief** keyword was added.
8.3(1)	The ACE show pattern to display ACL timestamp was modified.
9.14(1)	The **numeric** and **element-count** keywords were added.
9.17(1)	The command is now supported in the system context, which shows the element count of all access lists configured in all contexts. In addition, the element-count output includes the breakdown of object groups if object-group search is enabled.

Usage Guidelines

You can specify the **brief** keyword to display access list hit count, identifiers, and timestamp information in hexadecimal format. The configuration identifiers displayed in hexadecimal format are presented in three columns, and they are the same identifiers used in syslogs 106023 and 106100.

If an access list has been changed recently, the list is excluded from the output. A message will indicate when this happens.

Note The output shows how many elements are in the ACL. This number is not necessarily the same as the number of access control entries (ACE) in the ACL. The system might create extra elements when you use network objects with address ranges, for example, and these extra elements are not included in the output.

Clustering Guidelines

When using ASA clustering, if traffic is received by a single unit, the other units may still show a hit count for the ACL due to the clustering director logic. This is an expected behavior. Because the unit that did not receive any packets directly from the client may receive forwarded packets over the cluster control link for an owner request, the unit may check the ACL before sending the packet back to the receiving unit. As a result, the ACL hit count will be increased even though the unit did not pass the traffic.

Examples

The following examples show brief information about the specified access policy in hexadecimal format (ACEs in which the hitcount is not zero). The first two columns display identifiers in hexadecimal format, the third column lists the hit count, and the fourth column displays the timestamp value, also in hexadecimal format. The hit count value represents the number of times the rule has been hit by traffic. The timestamp value reports the time of the last hit. If the hit count is zero, no information is displayed.

The following is sample output from the **show access-list** command and shows the access list name “test,” which is applied on an outside interface in the “IN” direction:

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1 object-group
 D1 0x44ae5901
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq telnet (hitcnt=1) 0xca10ca21
  access-list test line 2 extended permit tcp 100.100.100.0 255.255.255.0 10.10.10.0
255.255.255.0 eq ssh(hitcnt=1) 0x5b704158
```

The following is sample output from the **show access-list** command when **object-group-search** group is not enabled:

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group BLK-LAN
 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=10) 0x30fe29a6
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=2) 0xce8596ec
   access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
```

```
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

The following is sample output from the **show access-list** command when **object-group-search** group is enabled:

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
(hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0) 0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
0xa52a0761
```

The following is sample output from the **show access-list brief** command when Telnet traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21
 44ae5901 00000001 4a68aa7e
```

The following is sample output from the **show access-list brief** command when SSH traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
ca10ca21 44ae5901 00000001 4a68aa7e
5b704158
 44ae5901 00000001 4a68aaa9
```

The following is sample output from the **show access-list** command and shows the access list name “test,” which is applied on an outside interface in the “IN” direction, with ACL Optimization enabled:

```
ciscoasa# show access-list test
access-list test; 3 elements; name hash: 0xcb4257a3
access-list test line 1 extended permit icmp any any (hitcnt=0) 0xb422e9c2
access-list test line 2 extended permit object-group TELNET-SSH object-group S1 object-group
 D1 0x44ae5901
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq
telnet (hitcnt=1) 0x7b1c1660
  access-list test line 2 extended permit tcp object-group S1(1) object-group D1(2) eq ssh
 (hitcnt=1) 0x3666f922
```

The following is sample output from the **show access-list brief** command when Telnet traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660
 44ae5901 00000001 4a68ab51
```

The following is sample output from the **show access-list brief** command when SSH traffic is passed:

```
ciscoasa (config)# sh access-list test brief
access-list test; 3 elements; name hash: 0xcb4257a3
7b1c1660 44ae5901 00000001 4a68ab51
3666f922
 44ae5901 00000001 4a68ab66
```

The following example shows the element count, which is the total number of access control entries for all access lists defined on the system. For access lists that are assigned as access groups, to control access globally or on an interface, you can reduce the element count by enabling object group search using the **object-group-search access-control** command. When object group search is enabled, network objects are used in the access control entries; otherwise, the objects are expanded into the individual IP addresses contained in the objects and separate entries are written for each source/destination address pair. Thus, a single rule that uses a source network object with 5 IP addresses, and a destination object with 6 addresses, would expand into 5 * 6 entries, 30 elements rather than one. The higher the element count, the larger the access lists, which can potentially impact performance.

```
asa(config)# show access-list element-count

Total number of access-list elements: 33934
```

Starting with 9.17(1), if you enable object-group search, additional information is presented about the number of object groups in the rules (OBJGRP), including the split between source (SRC OBJ) and destination (DST OBJ) objects, and the added and deleted groups.

```
ciscoasa/act/ciscoasactx001(config)# show access-list element-count
Total number of access-list elements: 892

OBJGRP      SRC OG      DST OG      ADD OG      DEL OG
842         842         842         842         0
```

In multiple context mode, if you use the element-count keyword in the system context, the statistics apply to all contexts, summarizing the count across the systems. If you enable object-group search, the information includes counts for total access control entries (ACE), objects (OBJGRP), and source (SRC) and destination (DST) object groups. If object-group search is disabled, the object counts will always be 0. The following example is for a system context when you have enabled object-group search.

```
ciscoasa/act(config)# show access-list element-count

Context Name             ACE        OBJGRP     SRC OG     DST OG
system                   0          0          0          0
admin                    0          0          0          0
ciscoasactx001           892        842        842        842
ciscoasactx002           312        298        298        298
ciscoasactx003           398        306        306        306
ciscoasactx004           162        132        132        132
ciscoasactx005           1280       583        583        583
ciscoasactx006           352        345        345        345
ciscoasactx007           353        351        351        351
ciscoasactx008           348        346        346        346
ciscoasactx009           433        420        420        420
ciscoasactx010           342        340        340        340
ciscoasactx011           363        361        361        361
```

```
ciscoasactx012          409        406        406        406
ciscoasactx013          381        373        373        373
ciscoasactx014          332        330        330        330
ciscoasactx015          465        374        374        374
ciscoasactx016          444        316        316        316
ciscoasactx017          284        268        268        268
sciscoasactx018         8837       0          0          0
ciscoasactx019          467        412        412        412
ciscoasactx020          934        527        527        527
ciscoasactx021          415        401        401        401
ciscoasactx022          676        562        562        562
ciscoasactx023          1208       1099       1099       1099
ciscoasactx024          350        322        322        322
ciscoasactx025          638        252        252        252
ciscoasactx026          318        304        304        304
ciscoasactx027          359        308        308        308
ciscoasactx028          1249       1087       1087       1087
ciscoasactx029          451        326        326        326
ciscoasactx030          377        315        315        315
ciscoasactx031          445        418        418        418
ciscoasactx032          347        309        309        309
ciscoasactx033          583        317        317        317
ciscoasactx034          340        311        311        311
ciscoasactx035          350        301        301        301

 Total access-list elements in all Context: 25894
```

Related Commands

Command	Description
access-list ethertype	Configures an access list that controls traffic based on its EtherType.
access-list extended	Adds an access list to the configuration and configures policy for IP traffic through the firewall.
clear access-list	Clears an access list counter.
clear configure access-list	Clears an access list from the running configuration.
show running-config access-list	Displays the current running access-list configuration.

show activation-key

To display the permanent license, active time-based licenses, and the running license, which is a combination of the permanent license and active time-based licenses. use the **show activation-key** command in privileged EXEC mode. For failover units, this command also shows the “Failover cluster” license, which is the combined keys of the primary and secondary units.

show activation-key [**detail**]

Syntax Description

detail	Shows inactive time-based licenses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(4)	The **detail** keyword was added.
8.2(1)	The output was modified to include additional licensing information.
8.3(1)	The output now includes whether a feature uses the permanent or time-based key, as well as the duration of the time-based key in use. It also shows all installed time-based keys, both active and inactive.
8.4(1)	Support for No Payload Encryption models was added.

Usage Guidelines

Some permanent licenses require you to reload the ASA after you activate them. <xref> lists the licenses that require reloading.

Table 2: Permanent License Reloading Requirements

Model	License Action Requiring Reload
All models	Downgrading the Encryption license.
ASA Virtual	Downgrading the vCPU license.

If you need to reload, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

If you have a No Payload Encryption model, then when you view the license, VPN and Unified Communications licenses will not be listed.

Examples

Example 2-1 Standalone Unit Output for the show activation-key command

The following is sample output from the **show activation-key** command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as each active time-based license:

```
ciscoasa# show activation-key
Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual
This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

Example 2-2 Standalone Unit Output for show activation-key detail

The following is sample output from the **show activation-key detail** command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as the permanent license and each installed time-based license (active and inactive):

```
ciscoasa# show activation-key detail
Serial Number:  88810093382
```

```
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5505 Security Plus license.
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days
Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                  : 25     7 days
```

Example 2-3 Primary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the **show activation-key detail** command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.

- The primary unit permanent license.
- The primary unit installed time-based licenses (active and inactive).

```
ciscoasa# show activation-key detail
Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.
Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
            Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
```

```
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days
Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                  : 100        7 days
0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

Example 2-4 Secondary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the **show activation-key detail** command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The "Failover Cluster" license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary unit permanent license.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

```
ciscoasa# show activation-key detail
Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
```

```
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
            Security Contexts            : 10             perpetual
            GTP/GPRS                     : Enabled        perpetual
            AnyConnect Premium Peers        : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
            Total UC Proxy Sessions      : 4              perpetual
            Botnet Traffic Filter        : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual
This platform has an ASA 5520 VPN Plus license.
Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-5 Standalone Unit Output for the ASA virtual without a License for show activation-key

The following output for a deployed 1 vCPU ASA virtual shows a blank activation key, an Unlicensed status, and a message to install a 1 vCPU license.

Note The command output shows, “This platform has an ASA virtual VPN Premium license.” This message specifies that the ASA virtual can perform payload encryption; it does not refer to the ASA virtual Standard vs. Premium licenses.

```
ciscoasa# **show activation-key**
Serial Number:  9APM1G4RV41
Running Permanent Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
ASAv Platform License State: Unlicensed
*Install 1 vCPU ASAv platform license for full functionality.
The Running Activation Key is not valid, using default settings:
Licensed features for this platform:
Virtual CPUs                      : 0              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
Failed to retrieve flash permanent activation key.
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-6 Standalone Unit Output for the ASA virtual with a 4 vCPU Standard License for show activation-key

Note The command output shows, “This platform has an ASA virtual VPN Premium license.” This message specifies that the ASA virtual can perform payload encryption; it does not refer to the ASA virtual Standard vs. Premium licenses.

```
ciscoasa# **show activation-key**

Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x0013e945 0x685a232c 0x1153fdac 0xeae8b068 0x4413f4ae
ASAv Platform License State: Compliant
Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
```

```
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-7 Standalone Unit Output for the ASA virtual with a 4 vCPU Premium License for show activation-key

Note The command output shows, “This platform has an ASA virtual VPN Premium license.” This message specifies that the ASA virtual can perform payload encryption; it does not refer to the ASA virtual Standard vs. Premium licenses.

```
ciscoasa# show activation-key
Serial Number:  9ALQ8W1XCJ7
Running Permanent Activation Key: 0x8224dd7d 0x943ed77c 0x9d71cdd0 0xd90474d0 0xcb04df82
ASAv Platform License State: Compliant
Licensed features for this platform:
Virtual CPUs                      : 4              perpetual
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 200            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 750            perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
UC Phone Proxy Sessions           : 1000           perpetual
Total UC Proxy Sessions           : 1000           perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Enabled        perpetual
Cluster                           : Disabled       perpetual
This platform has an ASAv VPN Premium license.
The flash permanent activation key is the SAME as the running permanent key.
ciscoasa#
```

Example 2-8 Primary Unit Output for the ASA Services Module in a Failover Pair for show activation-key

The following is sample output from the **show activation-key** command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).

- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The primary unit installed time-based licenses (active and inactive).

```
ciscoasa# show activation-key
erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

Example 2-9 Secondary Unit Output for the ASA Services Module in a Failover Pair for show activation-key

The following is sample output from the **show activation-key** command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the ASA. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

```
ciscoasa# show activation-key detail
Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683
Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
```

```
GTP/GPRS                          : Disabled       perpetual
Botnet Traffic Filter             : Disabled       perpetual
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 50             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
The flash permanent activation key is the SAME as the running permanent key.
```

Example 2-10 Output in a Cluster for show activation-key

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9
 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
 This platform has an ASA 5585-X base license.
 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual
 This platform has an ASA 5585-X base license.
 The flash permanent activation key is the SAME as the running permanent key.
Serial Number:  JMX1232L11M
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Running Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited  perpetual
Maximum VLANs                : 50         perpetual
Inside Hosts                 : Unlimited  perpetual
Failover                     : Disabled   perpetual
VPN-DES                      : Enabled    perpetual
VPN-3DES-AES                 : Enabled    perpetual
Security Contexts            : 0          perpetual
GTP/GPRS                     : Disabled   perpetual
SSL VPN Peers                : 2          perpetual
Total VPN Peers              : 250        perpetual
Shared License               : Disabled   perpetual
AnyConnect for Mobile        : Disabled   perpetual
AnyConnect for Linksys phone : Disabled   perpetual
AnyConnect Essentials        : Enabled    perpetual
Advanced Endpoint Assessment : Disabled   perpetual
UC Phone Proxy Sessions      : 12         62 days
Total UC Proxy Sessions      : 12         62 days
Botnet Traffic Filter        : Enabled    646 days

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
SSL VPN Peers           : 100         108 days
```

Related Commands

Command	Description
activation-key	Changes the activation key.

show ad-groups

To display groups that are listed on an Active Directory server, use the **show ad-groups** command in privileged EXEC mode:

show ad-groups *name* [**filter** *string*]

Syntax Description

name	The name of the Active Directory server group to query.
string	A string within quotes specifying all or part of the group name to search for.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.

Usage Guidelines

The show ad-groups command applies only to Active Directory servers that use the LDAP protocol to retrieve groups. Use this command to display AD groups that you can use for dynamic access policy AAA selection criteria.

When the LDAP attribute type = LDAP, the default time that the ASA waits for a response from the server is 10 seconds. You can adjust this time using the **group-search-timeout** command in aaa-server host configuration mode.

Note If the Active Directory server has a large number of groups, the output of the **show ad-groups command** may be truncated based on limitations of the amount of data the server can fit into a response packet. To avoid this problem, use the **filter** option to reduce the number of groups reported by the server.

Examples

```
ciscoasa# show ad-groups LDAP-AD17
            Server Group    LDAP-AD17

            Group list retrieved successfully
```

```
Number of Active Directory Groups       46

Account Operators

Administrators

APP-SSL-VPN CIO Users

Backup Operators

Cert Publishers

CERTSVC_DCOM_ACCESS

Cisco-Eng

DHCP Administrators

DHCP Users

Distributed COM Users

DnsAdmins

DnsUpdateProxy

Doctors

Domain Admins

Domain Computers

Domain Controllers

Domain Guests

Domain Users

Employees

Engineering

Engineering1

Engineering2

Enterprise Admins

Group Policy Creator Owners

Guests

HelpServicesGroup
```

The next example shows the same command with the **filter** option:

```
ciscoasa(config)# show ad-groups LDAP-AD17 filter “Eng”
.

Server Group    LDAP-AD17
```

```
Group list retrieved successfully

Number of Active Directory Groups       4

Cisco-Eng

Engineering

Engineering1

Engineering2
```

Related Commands

Command	Description
ldap-group-base-dn	Specifies a level in the Active Directory hierarchy where the server begins searching for groups that are used by dynamic group policies.
group-search-timeout	Adjusts the time the ASA waits for a response from an Active Directory server for a list of groups.

show admin-context

To display the context name currently assigned as the admin context, use the **show admin-context** command in privileged EXEC mode.

show admin-context

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show admin-context** command. The following example shows the admin context called "admin" and stored in the root directory of flash:

```
ciscoasa# show admin-context
Admin: admin flash:/admin.cfg
```

Related Commands

Command	Description
admin-context	Sets the admin context.
changeto	Changes between contexts or the system execution space.
clear configure context	Removes all contexts.
mode	Sets the context mode to single or multiple.
show context	Shows a list of contexts (system execution space) or information about the current context.

show alarm settings

To display the configuration for each type of alarm in the ISA 3000, use the **show alarm settings** command in user EXEC mode.

show alarm settings

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Examples

The following is a sample output from the **show alarm settings** command:

```
ciscoasa> show alarm settings

Power Supply
         Alarm                    Disabled
         Relay                    Disabled
         Notifies                 Disabled
         Syslog                   Disabled
Temperature-Primary
         Alarm                    Enabled
         Thresholds               MAX: 92C                 MIN: -40C
         Relay                    Enabled
         Notifies                 Enabled
         Syslog                   Enabled
Temperature-Secondary
         Alarm                    Disabled
         Threshold
         Relay                    Disabled
         Notifies                 Disabled
         Syslog                   Disabled
Input-Alarm 1
         Alarm                    Enabled
         Relay                    Disabled
         Notifies                 Disabled
         Syslog                   Enabled
```

```
Input-Alarm 2
        Alarm                   Enabled
        Relay                   Disabled
        Notifies                Disabled
        Syslog                  Enabled
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show environment alarm-contact	Displays all external alarm settings.
show facility-alarm relay	Displays relay in activated state.
show facility-alarm status	Displays all triggered alarms, or alarms based on severity specified.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

show arp

To view the ARP table, use the **show arp** command in privileged EXEC mode.

show arp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	Dynamic ARP age was added to the display.

Usage Guidelines

The display output shows dynamic, static, and proxy ARP entries. Dynamic ARP entries include the age of the ARP entry in seconds. Static ARP entries include a dash (-) instead of the age, and proxy ARP entries state "alias."

Examples

The following is sample output from the **show arp** command. The first entry is a dynamic entry aged 2 seconds. The second entry is a static entry, and the third entry is from proxy ARP.

```
ciscoasa# show arp
        outside 10.86.194.61 0011.2094.1d2b 2
        outside 10.86.194.1 001a.300c.8000 -
        outside 10.86.195.2 00d0.02a8.440a alias
```

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	Inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.

Command	Description
show running-config arp	Shows the current configuration of the ARP timeout.

show arp-inspection

To view the ARP inspection setting for each interface, use the **show arp-inspection** command in privileged EXEC mode.

show arp-inspection

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	Support for routed mode was added.

Examples

The following is sample output from the **show arp-inspection** command:

```
ciscoasa# show arp-inspection
interface                arp-inspection         miss
----------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

The **miss** column shows the default action to take for non-matching packets when ARP inspection is enabled, either “flood” or “no-flood.”

Related Commands

Command	Description
arp	Adds a static ARP entry.
arp-inspection	Inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics.
show arp statistics	Shows ARP statistics.

Command	Description
show running-config arp	Shows the current configuration of the ARP timeout.

show arp rate-limit

To show the ARP rate limit setting, use the **show arp rate-limit** command in privileged EXEC mode.

show arp rate-limit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Use this command to view the **arp rate-limit** setting.

Examples

The following example shows the ARP rate as 10000 per second:

```
ciscoasa# show arp rate-limit
arp rate-limit 10000
```

Related Commands

Command	Description
arp rate-limit	Sets the ARP rate limit.

show arp statistics

To view ARP statistics, use the show arp statistics command in privileged EXEC mode.

show arp statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show arp statistics** command:

```
ciscoasa# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

Table 2 shows each field description.

Table 3: show arp statistics Fields

Field	Description
Number of ARP entries	The total number of ARP table entries.
Dropped blocks in ARP	The number of blocks that were dropped while IP addresses were being resolved to their corresponding hardware addresses.

Field	Description
Maximum queued blocks	The maximum number of blocks that were ever queued in the ARP module, while waiting for the IP address to be resolved.
Queued blocks	The number of blocks currently queued in the ARP module.
Interface collision ARPs received	The number of ARP packets received at all ASA interfaces that were from the same IP address as that of an ASA interface.
ARP-defense gratuitous ARPs sent	The number of gratuitous ARPs sent by the ASA as part of the ARP-Defense mechanism.
Total ARP retries	The total number of ARP requests sent by the ARP module when the address was not resolved in response to first ARP request.
Unresolved hosts	The number of unresolved hosts for which ARP requests are still being sent out by the ARP module.
Maximum unresolved hosts	The maximum number of unresolved hosts that ever were in the ARP module since it was last cleared or the ASA booted up.

Related Commands

Command	Description
arp-inspection	Inspects ARP packets to prevent ARP spoofing.
clear arp statistics	Clears ARP statistics and resets the values to zero.
show arp	Shows the ARP table.
show running-config arp	Shows the current configuration of the ARP timeout.

show arp vtep-mapping

To display MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses, use the **show arp vtep-mapping** command in privileged EXEC mode.

show arp vtep-mapping

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

When the ASA sends a packet to a device behind a peer VTEP, the ASA needs two important pieces of information:

- The destination MAC address of the remote device
- The destination IP address of the peer VTEP

There are two ways in which the ASA can find this information:

- A single peer VTEP IP address can be statically configured on the ASA.

You cannot manually define multiple peers.

The ASA then sends a VXLAN-encapsulated ARP broadcast to the VTEP to learn the end node MAC address.

- A multicast group can be configured on each VNI interface (or on the VTEP as a whole).

The ASA sends a VXLAN-encapsulated ARP broadcast packet within an IP multicast packet through the VTEP source interface. The response to this ARP request enables the ASA to learn both the remote VTEP IP address along with the destination MAC address of the remote end node.

The ASA maintains a mapping of destination MAC addresses to remote VTEP IP addresses for the VNI interfaces.

Examples

See the following output for the **show arp vtep-mapping** command:

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

show asdm history

To display the contents of the ASDM history buffer, use the **show asdm history** command in privileged EXEC mode.

show asdm history [**view** *timeframe*] [**snapshot**] [**feature** *feature*] [**asdmclient**]

Syntax Description

asdmclient	(Optional) Displays the ASDM history data formatted for the ASDM client.
feature *feature*	(Optional) Limits the history display to the specified feature. The following are valid values for the *feature* argument: • **all** —Displays the history for all features (default). • **blocks** —Displays the history for the system buffers. • **cpu** —Displays the history for CPU usage. • **failover** —Displays the history for failover. • **ids** —Displays the history for IDS. • **interface** *if_name* —Displays the history for the specified interface. The *if_name* argument is the name of the interface as specified by the **nameif** command. • **memory** —Displays memory usage history. • **perfmon** —Displays performance history. • **sas** —Displays the history for Security Associations. • **tunnels** —Displays the history for tunnels. • **xlates** —Displays translation slot history.
snapshot	(Optional) Displays only the last ASDM history data point.
view *timeframe*	(Optional) Limits the history display to the specified time period. Valid values for the *timeframe* argument are: • **all** —all contents in the history buffer (default). • **12h** —12 hours • **5d** —5 days • **60m** —60 minutes • **10m** —10 minutes

Command Default

If no arguments or keywords are specified, all history information for all features is displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm history** command to the **show asdm history** command.

Usage Guidelines

The **show asdm history** command displays the contents of the ASDM history buffer. Before you can view ASDM history information, you must enable ASDM history tracking using the **asdm history enable** command.

Examples

The following is sample output from the **show asdm history** command. It limits the output to data for the outside interface collected during the last 10 minutes.

```
ciscoasa# show asdm history view 10m feature interface outside
Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
```

```
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
ciscoasa#
```

The following is sample output from the **show asdm history** command. Like the previous example, it limits the output to data for the outside interface collected during the last 10 minutes. However, in this example the output is formatted for the ASDM client.

```
ciscoasa# show asdm history view 10m feature interface outside asdmclient
MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|62464|
62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542|62547|
62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|62628|62633|
62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|62704|62711|62718|
62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
...
```

The following is sample output from the **show asdm history** command using the **snapshot** keyword:

```
ciscoasa# show asdm history view 10m snapshot
Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
```

```
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
```

```
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPsec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
ciscoasa#
```

Related Commands

Command	Description
asdm history enable	Enables ASDM history tracking.

show asdm image

To the current ASDM software image file, use the show **asdm image** command in privileged EXEC mode.

show asdm image

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm image** command to the **show asdm image** command.

Examples

The following is sample output from the **show asdm image** command:

```
ciscoasa# show asdm image
Device Manager image file, flash:/ASDM
```

Related Commands

Command	Description
asdm image	Specifies the current ASDM image file.

show asdm log_sessions

To display a list of active ASDM logging sessions and their associated session IDs, use the **show asdm log_sessions** command in privileged EXEC mode.

show asdm log_sessions

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Each active ASDM session has one or more associated ASDM logging sessions. ASDM uses the logging session to retrieve syslog messages from the ASA. Each ASDM logging session is assigned a unique session ID. You can use this session ID with the **asdm disconnect log_session** command to terminate the specified session.

Note Because each ASDM session has at least one ASDM logging session, the output for the **show asdm sessions** and **show asdm log_sessions** may appear to be the same.

Examples

The following is sample output from the **show asdm log_sessions** command:

```
ciscoasa# show asdm log_sessions
0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect log_session	Terminates an active ASDM logging session.

show asdm sessions

To display a list of active ASDM sessions and their associated session IDs, use the **show asdm sessions** command in privileged EXEC mode.

show asdm sessions

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was changed from the **show pdm sessions** command to the **show asdm sessions** command.

Usage Guidelines

Each active ASDM session is assigned a unique session ID. You can use this session ID with the **asdm disconnect** command to terminate the specified session.

Examples

The following is sample output from the **show asdm sessions** command:

```
ciscoasa# show asdm sessions
0 192.168.1.1
1 192.168.1.2
```

Related Commands

Command	Description
asdm disconnect	Terminates an active ASDM session.

show asp – show az

show as-path-access-list

To display the contents of all current autonomous system (AS) path access lists, use the show as-path-access-list command in user EXEC or privileged EXEC mode

show as-path-access-list [*name*]

Syntax Description

name	(Optional) Specifies the AS path access list name..

Command Default

If the name argument is not specified, command output is displayed for all AS path access lists.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Examples

The following is sample output from the show as-path-access-list command:

```
ciscoasa# show as-path-access-list
AS path access list as-path-acl-1
    deny RTR$
AS path access list as-path-acl-2
    permit 100$
```

<xref> shows each field description.

Table 4: show as-path-access-list Fields

Field	Description
AS path access list	Indicates the AS path access list name.
deny	Indicates the number of packets that are rejected since the regular expression failed to match the representation of the AS path of the route as an ASCII string.
permit	Indicates the number of packets that are forwarded since the regular expression matched the representation of the AS path of the route as an ASCII string.

show asp cluster counter

To debug global or context-specific information in a clustering environment, use the **show asp cluster counter** command in privileged EXEC mode.

show asp cluster counter

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show asp cluster counter** command shows the global and context-specific DP counters, which might help you troubleshoot a problem. This information is used for debugging purposes only, and the information output is subject to change. Consult the Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp cluster counter** command:

```
ciscoasa# show asp cluster counter
Global dp-counters:
Context specific dp-counters:
MCAST_FP_TO_SP                  361136
MCAST_SP_TOTAL                  361136
MCAST_SP_PKTS                   143327
MCAST_SP_PKTS_TO_CP             143327
MCAST_FP_CHK_FAIL_NO_HANDLE     217809
MCAST_FP_CHK_FAIL_NO_ACCEPT_IFC 81192
MCAST_FP_CHK_FAIL_NO_FP_FWD     62135
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp dispatch

To display statistics for the device’s load balance ASP dispatcher, which is useful for diagnosing performance issues, use the **show asp dispatch** command in privileged EXEC mode. It is only available for a firewall device in the hybrid poll/interrupt mode.

show asp dispatch

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.6(2)	This command was introduced.

Examples

The following is sample output from the **show asp dispatch** command.

```
ciscoasa# show asp dispatch
==== Lina DP thread dispatch stats - CORE 0 ====
Dispatch loop count         :          92260212
Dispatch C2C poll count     :                 2
CP scheduler busy           :          14936242
CP scheduler idle           :          77323971
RX ring busy                :           1513632
Async lock global q busy    :            809481
Global timer q busy         :           1958684
SNP flow bulk sync busy     :               174
Purg process busy           :              2838
Block attempts              :          44594355
Maximum timeout specified   :          10000000
Minimum timeout specified   :           1572864
Average timeout specified   :           9999994
Waken up with OK status     :           2476791
Waken up with timeout       :          42117564
Sleep interrupted           :             85753
Number of interrupts        :           2492566
Number of RX interrupts     :           1454442
Number of TX interrupts     :           2492566
Enable interrupt ok         :         174566236
Disable interrupt ok        :         174231423
```

```
Maximum elapsed time       :         54082257
Minimum elapsed time       :             6165
Average elapsed time       :          9658532
Message pipe stats         :

Last clearing of asp dispatch: Never

==== Lina DP thread home-ring/interface list - CORE 0 ====
Interface Internal-Data0/0: port-id 0 irq 10 fd 37
Interface GigabitEthernet0/0: port-id 256 irq 5 fd 38
Interface GigabitEthernet0/1: port-id 512 irq 9 fd 39
Interface GigabitEthernet0/2: port-id 768 irq 11 fd 40
>
```

show asp drop

To debug the accelerated security path dropped packets or connections, use the **show asp drop** command in privileged EXEC mode.

show asp drop [**flow** [*flow_drop_reason*] | **frame** [*frame_drop_reason*]]

Syntax Description

flow [*flow_drop_reason*]	(Optional) Shows the dropped flows (connections). You can specify a particular reason by using the *flow_drop_reason* argument. Use ? to see a list of possible flow drop reasons.
frame [*frame_drop_reason*]	(Optional) Shows the dropped packets. You can specify a particular reason by using the *frame_drop_reason* argument. Use ? to see a list of possible frame drop reasons.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.0(8)/7.2(4)/8.0(4)	Output includes a timestamp indicating when the counters were last cleared (see the **clear asp drop** command). It also displays the drop reason keywords next to the description, so you can easily use the **capture asp-drop** command with the associated keyword.

Usage Guidelines

The **show asp drop** command shows the packets or connections dropped by the accelerated security path, which might help you troubleshoot a problem. See the general operations configuration guide for more information about the accelerated security path. This information is used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

For detailed descriptions of each drop reason name and description, including recommendations, see show asp drop Command Usage .

Examples

The following is sample output from the **show asp drop** command, with the time stamp indicating the last time the counters were cleared:

```
ciscoasa# show asp drop
Frame drop:
  Flow is denied by configured rule (acl-drop)                             3
  Dst MAC L2 Lookup Failed (dst-l2_lookup-fail)                         4110
  L2 Src/Dst same LAN port (l2_same-lan-port)                            760
  Expired flow (flow-expired)                                              1
Last clearing: Never
Flow drop:
  Flow is denied by access rule (acl-drop)                                24
  NAT failed (nat-failed)                                              28739
  NAT reverse path failed (nat-rpf-failed)                             22266
  Inspection failure (inspect-fail)                                    19433
Last clearing: 17:02:12 UTC Jan 17 2012 by enable_15
```

Related Commands

Command	Description
capture	Captures packets, including the option to capture packets based on an ASP drop code.
clear asp drop	Clears drop statistics for the accelerated security path.
show conn	Shows information about connections.

show asp event dp-cp

To debug the data path or control path event queues, use the **show asp event dp-cp** command in privileged EXEC mode.

show asp event dp-cp [**cxsc msg**]

Syntax Description

cxsc msg	(Optional) Identifies the CXSC event messages that are sent to the CXSC event queue.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.1(3)	A routing event queue entry was added.

Usage Guidelines

The **show asp event dp-cp** command shows the contents of the data path and control path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the data path and control path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp event dp-cp** command:

```
ciscoasa# show asp event dp-cp
DP-CP EVENT QUEUE                   QUEUE-LEN  HIGH-WATER
Punt Event Queue                            0        2048
Routing Event Queue                         0           1
Identity-Traffic Event Queue                0          17
General Event Queue                         0           0
Syslog Event Queue                          0        3192
Non-Blocking Event Queue                    0           4
Midpath High Event Queue                    0           0
Midpath Norm Event Queue                    0           0
SRTP Event Queue                            0           0
HA Event Queue                              0           3
Threat-Detection Event Queue                0           3
ARP Event Queue                             0           3
IDFW Event Queue                            0           0
```

```
CXSC Event Queue                           0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt              4005920          0   935295  3070625  4005920       4372
  inspect-sunrp   4005920          0   935295  3070625  4005920       4372
routing                77          0       77        0       77          0
arp-in                618          0      618        0      618          0
identity-traffic     1519          0     1519        0     1519          0
syslog               5501          0     5501        0     5501          0
threat-detection       12          0       12        0       12          0
ips-cplane           1047          0     1047        0     1047          0
ha-msg                520          0      520        0      520          0
cxsc-msg              127          0      127        0      127          0
```

show asp load-balance

To display a histogram of the load balancer queue sizes, use the **show asp load-balance** command in privileged EXEC mode.

show asp load-balance [**detail**]

Syntax Description

detail	(Optional) Shows detailed information about hash buckets.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.1(1)	This command was added.

Usage Guidelines

The **show asp load-balance** command might help you troubleshoot a problem. Normally a packet will be processed by the same core that pulled it in from the interface receive ring. However, if another core is already processing the same connection as the packet just received, then the packet will be queued to that core. This queuing can cause the load balancer queue to grow while other cores are idle. See the **asp load-balance per-packet** command for more information.

Examples

The following is sample output from the **show asp load-balance** command. The X-axis represents the number of packets queued in different queues. The Y-axis represents the number of load balancer hash buckets (not to be confused with the bucket in the histogram title, which refers to the histogram bucket) that has packets queued. To know the exact number of hash buckets having the queue, use the **detail** keyword.

```
ciscoasa# show asp load-balance
Histogram of 'ASP load balancer queue sizes'
  64 buckets sampling from 1 to 65 (1 per bucket)
  6 samples within range (average=23)
                   ASP load balancer queue sizes

  100 +
      |
      |
      |
S     |
a     |
m     |
p     |
l  10 +
e     |
s     |
      |
      |
      |                           #
      |   # #                     # #           #
      |   # #                     # #           #
      +---------+---------+---------+---------+---------+---------+----
                10        20        30        40        50        60


                          # of queued jobs per queue
```

The following is sample output from the **show asp load-balance detail** command.

```
ciscoasa# show asp load-balance detail
<Same histogram output as before with the addition of the following values for the histogram>
Data points:
<snip>
  bucket[1-1] = 0 samples
  bucket[2-2] = 0 samples
  bucket[3-3] = 0 samples
  bucket[4-4] = 1 samples
  bucket[5-5] = 0 samples
  bucket[6-6] = 1 samples
<snip>
  bucket[28-28] = 2 samples
  bucket[29-29] = 0 samples
  bucket[30-30] = 1 samples
<snip>
  bucket[41-41] = 0 samples
  bucket[42-42] = 1 samples
```

Related Commands

Command	Description
asp load-balance per-packet	Changes the core load balancing method for multi-core ASA models.

show asp load-balance per-packet

To display specific statistics for ASP load balancing per packet, use the **show asp load-balance per-packet** command in privileged EXEC mode.

show asp load-balance per-packet [**history**]

Syntax Description

history	(Optional) Shows the configuration status (enabled, disabled, or auto), current status (enabled or disabled), high and low watermarks, the global threshold, the number of times an automatic switch occurred, the minimum and maximum wait times with automatic switching enabled, the history of ASP load balancing per packet with time stamps, and the reasons for switching it on and off.

Command Default

If you do not specify any options, this command shows the basic status, related values, and statistics of ASP load balancing per packet.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(1)	This command was added.

Usage Guidelines

The **show asp load-balance per-packet** command shows the configuration status (enabled, disabled, or auto), current status (enabled or disabled), high and low watermarks, the global threshold, the number of times an automatic switch occurred, and the minimum and maximum wait times with automatic switching enabled, for ASP load balancing per packet.

The information appears in the following format:

```
Config mode    : [ enabled | disabled | auto ]
Current status : [ enabled | disabled ]
RX ring Blocks low/high watermark      : [RX ring Blocks low watermark in percentage] / [RX
 ring Blocks high watermark in percentage]
System RX ring count low threshold     : [System RX ring count low threshold] / [Total
number of RX rings in the system]
System RX ring count high threshold    : [System RX ring count high threshold] / [Total
number of RX rings in the system]
```

Auto mode

```
Current RX ring count threshold status : [Number of RX rings crossed watermark] / [Total
number of RX rings in the system]
```

```
Number of times auto switched          : [Number of times ASP load-balance per-packet has
been switched]
Min/max wait time with auto enabled    : [Minimal wait time with auto enabled] / [Maximal
wait time with auto enabled] (ms)
```

Manual mode

```
Current RX ring count threshold status : N/A
```

Only the ASA 5585-X and the ASASM support the use of this command.

Examples

The following is sample output from the **show asp load-balance per-packet** command:

```
ciscoasa# show asp load-balance per-packet
Config status  : auto
Current status : disabled
RX ring Blocks low/high watermark      : 50% / 75%
System RX ring count low threshold     : 1 / 33
System RX ring count high threshold    : 7 / 33
Current RX ring count threshold status : 0 / 33
Number of times auto switched          : 17
Min/max wait time with auto enabled    : 200 / 6400 (ms)
```

The following is sample output from the **show asp load-balance per-packet history** command:

ciscoasa# **show asp load-balance per-packet history**

Config status : auto

Current status : disabled

RX ring Blocks low/high watermark : 50% / 75%

System RX ring count low threshold : 1 / 33

System RX ring count high threshold : 7 / 33

Current RX ring count threshold status : 0 / 33

Number of times auto switched : 17

Min/max wait time with auto enabled : 200 / 6400 (ms)

==

From State To State Reason

==

15:07:13 UTC Dec 17 2013

Manually Disabled Manually Disabled Disabled at startup

15:09:14 UTC Dec 17 2013

Manually Disabled Manually Enabled Config

15:09:15 UTC Dec 17 2013

Manually Enabled Auto Disabled 0/33 of the ring(s) crossed the watermark

15:10:16 UTC Dec 17 2013

Auto Disabled Auto Enabled 1/33 of the ring(s) crossed the watermark

```
Internal-Data0/0 RX[01] crossed above high watermark
15:10:16 UTC Dec 17 2013
Auto Enabled Auto Enabled 2/33 of the ring(s) crossed the watermark
Internal-Data0/1 RX[04] crossed above high watermark
15:10:16 UTC Dec 17 2013
Auto Enabled Auto Enabled 3/33 of the ring(s) crossed the watermark
Internal-Data0/1 RX[05] crossed above high watermark
15:10:16 UTC Dec 17 2013
Auto Enabled Auto Enabled 2/33 of the ring(s) crossed the watermark
Internal-Data0/0 RX[01] dropped below low watermark
15:10:17 UTC Dec 17 2013
Auto Enabled Auto Enabled 3/33 of the ring(s) crossed the watermark
Internal-Data0/2 RX[01] crossed above high watermark
(---More---)
15:14:01 UTC Dec 17 2013
Auto Enabled Auto Disabled 8/33 of the ring(s) crossed the watermark
Internal-Data0/3 RX[01] crossed above high watermark
15:14:01 UTC Dec 17 2013
Auto Disabled Auto Enabled 7/33 of the ring(s) crossed the watermark
Internal-Data0/3 RX[01] dropped below low watermark
(---More---)
15:20:11 UTC Dec 17 2013
Auto Enabled Auto Disabled 0/33 of the ring(s) crossed the watermark
Internal-Data0/2 RX[01] dropped below low watermark
(---More---)
```

Related Commands

Command	Description
asp load-balance per-packet auto	Automatically switches ASP load balancing per packet on and off on each interface receive ring or set of flows.
clear asp load-balance history	Clears the history of ASP load balancing per packet and reset the number of times an automatic switch occurred.

show asp multiprocessor accelerated-features

To debug the accelerated security path multiprocessor accelerate, use the **show asp multiprocessor accelerated-features** command in privileged EXEC mode.

show asp multiprocessor accelerated-features

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.6(2)	This command was introduced.

Usage Guidelines

The **show asp multiprocessor accelerated-features** command shows the lists of features accelerated for multiprocessors, which might help you troubleshoot a performance problem.

Examples

The following is sample output from the **show asp multiprocessor accelerated-features** command:

```
ciscoasa# show asp multiprocessor accelerated-features
MultiProcessor accelerated feature list:
        Access Lists
        DNS Guard
        Failover Stateful Updates
        Flow Operations(create, update, and tear-down)
        Inspect HTTP URL Logging
        Inspect HTTP (AIC)
        Inspect IPSec Pass through
        Inspect ICMP and ICMP error
        Inspect RTP/RTCP
        IP Audit
        IP Fragmentation & Re-assembly
        IPSec data-path
        MPF L2-L4 Classify
        Multicast forwarding
        NAT/PAT
        Netflow using UDP transport
        Non-AIC Inspect DNS
        Packet Capture
        QOS
        Resource Management
        Routing Lookup
        Shun
        SSL data-path
        Syslogging using UDP transport
        TCP Intercept
        TCP Security Engine
        TCP Transport
        Threat Detection
        Unicast RPF
        WCCP Re-direct
Above list applies to routed, transparent, single and multi mode.
```

show asp overhead

To track and display spin lock and async loss statistics, use the **show asp overhead** command in privileged EXEC mode.

show asp overhead [**sort-by-average**] [**sort-by-file**]

Syntax Description

sort-by-average	Sorts the results by average cycles per call
sort-by-file	Sorts the results by filename

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.6(2)	This command was introduced.

Examples

The following is sample output from the **show asp overhead** command:

```
ciscoasa# show asp overhead
0.0% of available CPU cycles were lost to Multiprocessor overhead
        since last the MP overhead statistics were last cleared
              File Name Line Function Call            Avg         Cycles      %
----------------------- ---- ----------------------  -----  -------------  -----
```

show asp rule-engine

To see the status of the tmatch compilation process, use the **show asp rule-engine** command in privileged EXEC mode.

show asp rule-engine [**table classify** { **v4** | **v6** }]

Command History

Release	Modification
9.17(1)	This command was introduced.
9.18(1)	This command was enhanced to include more detailed information about each table regarding their rule-count and compilation status for IPv4 and IPv6.
9.20(1)	The duration information shows the split between the time compilation was done in the control place compared to the data path.

Example

The following example shows whether the compilation of an access list that is used as an access group is in progress or completed. Compilation time depends on the size of the access list. The time status of Start and Completed is common for all rules, because it is a batch process and not specific to modules. Most module element counts will be shown in the table. The status also shows NAT rules, routes, objects, and interface compilation.

```
ciscoasa# show asp rule-engine
Rule compilation Status:   Completed
Duration(ms):              352 (Control: 52, DATAPATH: 300)
Start Time:                17:56:05 UTC Apr 6 2021
Last Completed Time:       17:56:15 UTC Apr 6 2021
ACL Commit Mode:           MANUAL
Object Group Search:       DISABLED
Transitional Commit Model: DISABLED

Module    |  Insert   |  Remove   |  Current   |

 NAT      |       17  |        0  |        17  |
 ROUTE    |       51  |       12  |        39  |
 IFC      |        9  |        0  |         9  |
 ACL      |      426  |        5  |       421  |
```

Following example shows output of the **show asp rule-engine table classify ipv4** command when compilation is yet to begin:

```
firepower(config)# show asp rule-engine table classify v4

------------------------------------------------------------
Table name        | Rule-count      | Compilation status |
------------------------------------------------------------
v4 security       | 8565712         | pending for compile |
------------------------------------------------------------
v4 input          | 86              | Completed   |
------------------------------------------------------------
```

```
v4 input reverse  | 47             | Completed   |
------------------------------------------------------------
v4 output         | 36             | Completed   |
------------------------------------------------------------
v4 output reverse | 3              | Completed   |
------------------------------------------------------------
```

Following example shows output of the command when compilation is in progress:

```
firepower(config)# show asp rule-engine table classify v4
-----------------------------------------------------------
Table name        | Rule-count     | Compilation status |
-----------------------------------------------------------
v4 security       | 8565710        | in progress (39%) |
-----------------------------------------------------------
v4 input          | 86             | Completed   |
-----------------------------------------------------------
v4 input reverse  | 45             | Completed   |
-----------------------------------------------------------
v4 output         | 36             | Completed   |
-----------------------------------------------------------
v4 output reverse | 3              | Completed   |
-----------------------------------------------------------
```

Following example shows output of the command when compilation is complete:

```
firepower(config)# show asp rule-engine table classify v4
------------------------------------------------------------
Table name        | Rule-count     | Compilation status |
------------------------------------------------------------
v4 security       | 8565712        | Completed   |
------------------------------------------------------------
v4 input          | 86             | Completed   |
------------------------------------------------------------
v4 input reverse  | 47             | Completed   |
------------------------------------------------------------
v4 output         | 36             | Completed   |
------------------------------------------------------------
v4 output reverse | 3              | Completed   |
------------------------------------------------------------
```

show asp table cluster chash-table

To show the cluster hash tables, use the **show asp table cluster chash-table** command in privileged EXEC mode.

show asp table cluster chash-table

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

To localize the traffic within the same site using director localization, each cluster member unit maintains two additional cHash tables; one table contains all members in the local site, and the other contains all local members except the current unit.

Examples

The following is sample output from the **show asp table cluster chash-table** command. Site 1 has unit 0 and 2, and Site 2 has unit 1 and 3. From unit 0, it shows the following:

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0,
0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0,
0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 0, 0, 0, 2, 2, 2, 2, 2, 2, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 0, 0, 0, 2, 2, 2, 2, 0, 0, 0, 0,

Cluster backup chash table:
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,
2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2,

[...]
```

Related Commands

Command	Description
director-localization	Enables director localization.

show asp table arp

To debug the accelerated security path ARP tables, use the **show asp table arp** command in privileged EXEC mode.

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

Syntax Description

address *ip_address*	(Optional) Identifies an IP address for which you want to view ARP table entries.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the ARP table.
netmask *mask*	(Optional) Sets the subnet mask for the IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.8(2)	The command output was updated for “reference” information.

Usage Guidelines

The **show arp** command shows the contents of the control plane, while the **show asp table arp** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command. The reference value in the command output represents the number of flows for the specific entry,

Examples

The following is sample output from the **show asp table arp** command:

```
ciscoasa# show asp table arp
Context: single_vf, Interface: inside
  10.86.194.50                             Active   000f.66ce.5d46 hits 0 reference 0
  10.86.194.1                              Active   00b0.64ea.91a2 hits 638 reference 1
  10.86.194.172                            Active   0001.03cf.9e79 hits 0 reference 0
  10.86.194.204                         Active   000f.66ce.5d3c hits 0 reference 0
  10.86.194.188                         Active   000f.904b.80d7 hits 0 reference 0
Context: single_vf, Interface: identity
  ::                                    Active   0000.0000.0000 hits 0 reference 0
  0.0.0.0                               Active   0000.0000.0000 hits 50208 reference 5
```

Related Commands

Command	Description
show arp	Shows the ARP table.
show arp statistics	Shows ARP statistics.

show asp table classify

To debug the accelerated security path classifier tables, use the **show asp table classify** command in privileged EXEC mode.

show asp table classify [**interface** *interface_name*] [**crypto | domain** *domain_name*] [**hits**] [**match** *regexp*] [**user-statistics**]

Syntax Description

crypto	(Optional) Shows the encrypt, decrypt, and ipsec tunnel flow domains only.
domain *domain_name*	(Optional) Shows entries for a specific classifier domain. See the CLI help for a list of the available domains.
hits	(Optional) Shows classifier entries that have non-zero hits values.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the classifier table.
match *regexp*	(Optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.
user-statistics	(Optional) Specifies user and group information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(4)	The **hits** option and the timestamp were added to indicate the last time the ASP table counters were cleared.
8.0(2)	A new counter was added to show the number of times a match compilation was aborted. This counter is shown only if the value is greater than 0.
8.2(2)	The **match** *regexp* option was added.
8.4(4.1)	The **csxc** and **cxsc-auth-proxy** domains for the ASA CX module was added.

Release	Modification
9.0(1)	The **user-statistics** keyword was added. The output was updated to add security group names and source and destination tags.
9.2(1)	Added the sfr domain for the ASA FirePOWER module.
9.3(1)	The security group tag (SGT) value has been modified in the output. The tag value "tag=0" indicates an exact match to 0x0, which is the reserved SGT value for "unknown." The SGT value "tag=any" indicates a value that you do not need to consider in the rule.
9.6(2)	Added the **inspect-m3ua** domain.

Usage Guidelines

The **show asp table classify** command shows the classifier contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. The classifier examines properties of incoming packets, such as protocol, and source and destination address, to match each packet to an appropriate classification rule. Each rule is labeled with a classification domain that determines what types of actions are performed, such as dropping a packet or allowing it through. The information shown is used for debugging purposes only, and the output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table classify** command:

```
ciscoasa# show asp table classify
Interface test:
No. of aborted compiles for input action table 0x33b3d70: 29
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=10.86.194.60, mask=255.255.255.255, port=0, tag=any
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53, tag=any
        dst ip=0.0.0.0, mask=0.0.0.0, port=0, tag=any
...
```

The following is sample output from the **show asp table classify hits** command with a record of the last clearing hits counters:

```
Interface mgmt:
in id=0x494cd88, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
in id=0x494d1b8, priority=112, domain=permit, deny=false
hits=1, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1 src ip=0.0.0.0, mask=0.0.0.0,
 port=0 dst ip=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
Interface inside:
in id=0x48f1580, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
in id=0x48f09e0, priority=1, domain=permit, deny=false
hits=101, user_data=0x0, cs_id=0x0, l3_type=0x608 src mac=0000.0000.0000, mask=0000.0000.0000
 dst mac=0000.0000.0000, mask=0000.0000.0000
```

```
Interface outside:
in id=0x48c0970, priority=210, domain=permit, deny=true
hits=54, user_data=0x1, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip=0.0.0.0,
mask=0.0.0.0, port=0 dst ip=255.255.255.255, mask=255.255.255.255, port=0, dscp=0x0
```

The following is sample output from the **show asp table classify hits** command that includes Layer 2 information:

```
Input Table
in  id=0x7fff2de10ae0, priority=120, domain=permit, deny=false
 hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=1
 src ip/id=0.0.0.0, mask=0.0.0.0, icmp-type=0
 dst ip/id=0.0.0.0, mask=0.0.0.0, icmp-code=0, dscp=0x0
 input_ifc=LAN-SEGMENT, output_ifc=identity in  id=0x7fff2de135c0, priority=0,
domain=inspect-ip-options, deny=true
 hits=41, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
 src ip/id=0.0.0.0, mask=0.0.0.0, port=0
 dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, dscp=0x0
 input_ifc=LAN-SEGMENT, output_ifc=any
.
.
.
Output Table:
L2 - Output Table:
L2 - Input Table:
in  id=0x7fff2de0e080, priority=1, domain=permit, deny=false
 hits=30, user_data=0x0, cs_id=0x0, l3_type=0x608
 src mac=0000.0000.0000, mask=0000.0000.0000
 dst mac=0000.0000.0000, mask=0000.0000.0000
 input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e580, priority=1, domain=permit, deny=false
 hits=382, user_data=0x0, cs_id=0x0, l3_type=0x8
 src mac=0000.0000.0000, mask=0000.0000.0000
 dst mac=0000.0000.0000, mask=0100.0000.0000
 input_ifc=LAN-SEGMENT, output_ifc=any
in  id=0x7fff2de0e800, priority=1, domain=permit, deny=false
 hits=312, user_data=0x0, cs_id=0x0, l3_type=0x8
 src mac=0000.0000.0000, mask=0000.0000.0000
 dst mac=ffff.ffff.ffff, mask=ffff.ffff.ffff
 input_ifc=LAN-SEGMENT, output_ifc=any
```

The following is sample output from the **show asp table classify** command when a security group is not specified in the access list:

```
ciscoasa# show asp table classify
in  id=0x7ffedb54cfe0, priority=500, domain=permit, deny=true
        hits=0, user_data=0x6, cs_id=0x0, flags=0x0, protocol=0
        src ip/id=224.0.0.0, mask=240.0.0.0, port=0, tag=any
        dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
        input_ifc=management, output_ifc=any
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table cluster chash-table

To debug the accelerated security path cHash tables for clustering, use the **show asp table cluster chash-table** command in privileged EXEC mode.

show asp table cluster chash-table

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show asp table cluster chash-table** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table cluster chash-table** command:

```
ciscoasa# show asp table cluster chash-table
Cluster current chash table:
00003333
21001200
22000033
02222223
33331111
21110000
00133103
22222223
30000102
11222222
23222331
00002223
33111111
11000112
22332000
00231121
```

```
11222220
33330223
31013211
11101111
13111111
11023133
30001100
00000111
12022222
00133333
33222000
00022222
33011333
11110002
33333322
13333030
```

Related Commands

Command	Description
show asp cluster counter	Shows cluster datapath counter information.

show asp table cts sgt-map

To show the IP address-security group table mapping from the IP address-security group table database that is maintained in the data path for Cisco TrustSec, use the **show asp table cts sgt-map** command in privileged EXEC mode.

show asp table cts sgt-map [**address** *ipv4* [/ *mask*] | **address** *ipv6* [/ *prefix*] | **ipv4** | **ipv6** | **sgt** *sgt*]

Syntax Description

address {*ipv4* [/*mask*] /*ipv6* [/*prefix*]}	(Optional.) Shows only IP address-security group table mapping for the specific IPv4 or IPv6 address. Include an IPv4 subnet mask or IPv6 prefix to see the mapping for a network.
ipv4	(Optional) Shows all of the IP address-security group table mapping for IPv4 addresses.
ipv6	(Optional) Shows all of the IP address-security group table mapping for IPv6 addresses.
sgt *sgt*	(Optional) Shows the IP address-security group table mapping for the specified security group table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.
9.6(1)	The ability to show network mappings was added.

Usage Guidelines

If the address is not specified, then all the entries in the IP address-security group table database in the data path appear. In addition, the security group names appear when available.

Examples

The following is sample output from the **show asp table cts sgt-map** command:

```
ciscoasa# show asp table cts sgt-map
IP Address                         SGT
==================================================
10.10.10.5                         1234:Marketing
10.34.89.12                        5:Engineering
10.67.0.0\16                       338:HR
192.4.4.4                          345:Finance
Total number of entries shown = 4
```

The following is sample output from the **show asp table cts sgt-map address** command:

```
ciscoasa# show asp table cts sgt-map address 10.10.10.5
IP Address                         SGT
=================================================
10.10.10.5                         1234:Marketing
Total number of entries shown = 1
```

The following is sample output from the **show asp table cts sgt-map ipv6** command:

```
ciscoasa# show asp table cts sgt-map ipv6
IP Address                               SGT
=============================================================
FE80::A8BB:CCFF:FE00:110                 17:Marketing-Servers
FE80::A8BB:CCFF:FE00:120                 18:Eng-Servers
Total number of entries shown = 2
```

The following is sample output from the **show asp table cts sgt-map sgt** command:

```
ciscoasa# show asp table cts sgt-map sgt 17
IP Address                               SGT
==============================================
FE80::A8BB:CCFF:FE00:110                 17
Total number of entries shown = 1
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show asp table dynamic-filter

To debug the accelerated security path Botnet Traffic Filter tables, use the **show asp table dynamic-filter** command in privileged EXEC mode.

show asp table dynamic-filter [**hits**]

Syntax Description

hits	(Optional) Shows classifier entries which have non-zero hits values.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

The **show asp table dynamic-filter** command shows the Botnet Traffic Filter rules in the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table dynamic-filter** command:

```
ciscoasa# show asp table dynamic-filter
Context: admin
 Address 10.246.235.42 mask 255.255.255.255 name: example.info
flags: 0x44 hits 0
 Address 10.40.9.250 mask 255.255.255.255 name: bad3.example.com
flags: 0x44 hits 0
 Address 10.64.147.20 mask 255.255.255.255 name: bad2.example.com flags: 0x44
hits 0
 Address 10.73.210.121 mask 255.255.255.255 name: bad1.example.com flags:
0x44 hits 0
 Address 10.34.131.135 mask 255.255.255.255 name: bad.example.com flags:
0x44 hits 0
 Address 10.64.147.16 mask 255.255.255.255 name:
1st-software-downloads.com flags: 0x44 hits 2
 Address 10.131.36.158 mask 255.255.255.255 name: www.example.com flags: 0x41 hits 0
 Address 10.129.205.209 mask 255.255.255.255 flags: 0x1 hits 0
 Address 10.166.20.10 mask 255.255.255.255 flags: 0x1 hits 0
...
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.

Command	Description
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show asp table filter

To debug the accelerated security path filter tables, use the **show asp table filter** command in privileged EXEC mode.

show asp table filter [**access-list** *acl-name*] [**hits**] [**match** *regexp*]

Syntax Description

acl-name	(Optional) Specifies the installed filter for a specified access list.
hits	(Optional) Specifies the filter rules that have non-zero hits values.
match *regexp*	(optional) Shows classifier entries that match the regular expression. Use quotes when regular expressions include spaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

When a filter has been applied to a VPN tunnel, the filter rules are installed into the filter table. If the tunnel has a filter specified, then the filter table is checked before encryption and after decryption to determine whether the inner packet should be permitted or denied.

Examples

The following is sample output from the **show asp table filter** command before a user1 connects. Only the implicit deny rules are installed for IPv4 and IPv6 in both the inbound and outbound directions.

```
ciscoasa# show asp table filter
Global Filter Table:
 in  id=0xd616ef20, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd613ea60, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f420, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd615ef70, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
 out id=0xd616f1a0, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd614d900, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd616f6d0, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd6161638, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
```

The following is sample output from the **show asp table filter** command after a user1 has connected. VPN filter ACLs are defined based on the inbound direction—the source represents the peer and the destination represents inside resources. The outbound rules are derived by swapping the source and destination for the inbound rule.

```
ciscoasa# show asp table filter
Global Filter Table:
 in  id=0xd682f4a0, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd682f460, filter_id=0x2(vpnfilter), protocol=6
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=21
 in  id=0xd68366a0, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd6d89050, filter_id=0x2(vpnfilter), protocol=6
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=5001
 in  id=0xd45d5b08, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd45d5ac8, filter_id=0x2(vpnfilter), protocol=17
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=5002
 in  id=0xd6244f30, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd6244ef0, filter_id=0x2(vpnfilter), protocol=1
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=95.1.224.100, mask=255.255.255.255, port=0
 in  id=0xd64edca8, priority=12, domain=vpn-user, deny=true
         hits=0, user_data=0xd64edc68, filter_id=0x2(vpnfilter), protocol=1
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f018, priority=11, domain=vpn-user, deny=true
         hits=43, user_data=0xd613eb58, filter_id=0x0(-implicit deny-), protocol=0
         src ip=0.0.0.0, mask=0.0.0.0, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 in  id=0xd616f518, priority=11, domain=vpn-user, deny=true
         hits=0, user_data=0xd615f068, filter_id=0x0(-implicit deny-), protocol=0
         src ip=::/0, port=0
         dst ip=::/0, port=0
 out id=0xd7395650, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd7395610, filter_id=0x2(vpnfilter), protocol=6
         src ip=95.1.224.100, mask=255.255.255.255, port=21
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d49b8, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd45d4978, filter_id=0x2(vpnfilter), protocol=6
         src ip=95.1.224.100, mask=255.255.255.255, port=5001
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd45d5cf0, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd45d5cb0, filter_id=0x2(vpnfilter), protocol=17
         src ip=95.1.224.100, mask=255.255.255.255, port=5002
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd6245118, priority=12, domain=vpn-user, deny=false
         hits=0, user_data=0xd62450d8, filter_id=0x2(vpnfilter), protocol=1
         src ip=95.1.224.100, mask=255.255.255.255, port=0
         dst ip=0.0.0.0, mask=0.0.0.0, port=0
 out id=0xd64ede90, priority=12, domain=vpn-user, deny=true
         hits=0, user_data=0xd64ede50, filter_id=0x2(vpnfilter), protocol=1
         src ip=0.0.0.0, mask=0.0.0.0, port=0
```

```
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f298, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd614d9f8, filter_id=0x0(-implicit deny-), protocol=0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
out id=0xd616f7c8, priority=11, domain=vpn-user, deny=true
        hits=0, user_data=0xd6161730, filter_id=0x0(-implicit deny-), protocol=0
        src ip=::/0, port=0
        dst ip=::/0, port=0
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.
show asp table classifier	Shows the classifier contents of the accelerated security path.

show asp table interfaces

To debug the accelerated security path interface tables, use the **show asp table interfaces** command in privileged EXEC mode.

show asp table interfaces

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show asp table interfaces** command shows the interface table contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table interfaces** command:

```
ciscoasa# show asp table interfaces
** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20
Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20
Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20
```

```
Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show asp table network-service

To debug the accelerated security path network-service object tables, use the **show asp table network-service** command in privileged EXEC mode.

show asp table network-service

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.17(1)	This command was introduced.

Example

The following example shows how to display the network-service object table:

```
ciscoasa# show asp table network-service
Per-Context Category NSG:
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=214491, branch_name=connect.facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=370809, branch_name=facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=490321, branch_name=fbcdn.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=548791, branch_name=fbcdn-photos-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=681143, branch_name=fbcdn-photos-e-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

```
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=840741, branch_name=fbcdn-photos-b-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1014669, branch_name=fbstatic-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1098051, branch_name=fbexternal-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1217875, branch_name=fbcdn-profile-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1379985, branch_name=fbcdn-creative-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1524617, branch_name=channel.facebook.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1683343, branch_name=fbcdn-dragon-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1782703, branch_name=contentcache-a.akamaihd.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=1868733, branch_name=facebook.net.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2068293, branch_name=plus.google.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2176667, branch_name=instagram.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, source, domain, nsg_id=512, hits=0
        subnet=0.0.0.0/0, branch_id=2317259, branch_name=linkedin.com.,
ip_prot=0, port=0/0x0, destination, domain, nsg_id=1, hits=0
```

show asp table routing management-only

To debug the accelerated security path routing tables, use the **show asp table routing** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses. The management-only keyword, displays the number portability routes in the management routing table.

show asp table routing [**input | output**] [**address** *ip_address* [**netmask** *mask*] | **interface** *interface_name*] **management-only**

Syntax Description

address *ip_address*	Sets the IP address for which you want to view routing entries. For IPv6 addresses, you can include the subnet mask as a slash (/) followed by the prefix (0 to 128). For example, enter the following: `fe80::2e0:b6ff:fe01:3b7a/128`
input	Shows the entries from the input route table.
interface *interface_name*	(Optional) Identifies a specific interface for which you want to view the routing table.
netmask *mask*	For IPv4 addresses, specifies the subnet mask.
output	Shows the entries from the output route table.
management-only	Shows the number portability routes in the management routing table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	Routing per zone information was added.
9.5(1)	The management-only keyword to support management routing table was added.

Usage Guidelines

The **show asp table routing** command shows the routing table contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command. The management-only keyword, displays the number-portability routes in the management routing table.

Note Invalid entries may appear in the show asp table routing command output on the ASA 5505.

Examples

The following is sample output from the **show asp table routing** command:

```
ciscoasa# show asp table routing
in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

Note Invalid entries in the **show asp table routing** command output may appear on the ASA 5505 platform. Ignore these entries; they have no effect.

Related Commands

Command	Description
show route	Shows the routing table in the control plane.

show asp table socket

To help debug the accelerated security path socket information, use the show asp table socket command in privileged EXEC mode.

show asp table socket [**socket | handle**] [**stats**]

Syntax Description

socket handle	Specifies the length of the socket.
stats	Shows the statistics from the accelerated security path socket table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The show asp table socket command shows the accelerated security path socket information, which might help in troubleshooting accelerated security path socket problems. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table socket** command.

```
Protocol  Socket    Local Address               Foreign Address         State
TCP       00012bac  10.86.194.224:23            0.0.0.0:*               LISTEN
TCP       0001c124  10.86.194.224:22            0.0.0.0:*               LISTEN
SSL       00023b84  10.86.194.224:443           0.0.0.0:*               LISTEN
SSL       0002d01c  192.168.1.1:443             0.0.0.0:*               LISTEN
DTLS      00032b1c  10.86.194.224:443           0.0.0.0:*               LISTEN
SSL       0003a3d4  0.0.0.0:443                 0.0.0.0:*               LISTEN
DTLS      00046074  0.0.0.0:443                 0.0.0.0:*               LISTEN
TCP       02c08aec  10.86.194.224:22            171.69.137.139:4190     ESTAB
```

The following is sample output from the **show asp table socket** with handle command.

```
docs-bxb-asa1/NoCluster/actNoFailover# show asp table socket 123456
Statistics for socket 0x00123456:
```

```
2) AM Module
   Mod handle: 0x000000000040545a
   Rx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/3  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        App Flow-Ctrl Tx: 0
        Stack:          0x00007fac1cb539c0
        New Conn Cb:    0x0000560fabeeb110
        Notify   Cb:    0x0000560fabeeb500
        App Hdl:        0x00007fac28dcb150
        Shared  Lock:   0x00007fac1685a280
          Group Lock:   0x00007fac1685a280
          Async Lock:   0x00007fac13099640
        Closed Mod Rx: -1, Tx: 3
        Push Module:    INVALID
        State:          LISTEN
        Flags: 0x0
          none
1) SSL Module
   Mod handle: 0x0000000000xxxxxx
   Rx:  0/10 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/10 ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        Upstream Active/peak/total:     0/0/0
        Downstream Active/peak/total:   0/0/0
        Inbound bytes rx/tx:    0/0
        Inbound packets rx/tx:  0/0
        Inbound packets lost:   0
        Outbound bytes rx/tx:   0/0
        Outbound packets rx/tx: 0/0
        Outbound packets lost:  0
        Upstream Close Attempt:         0
        Upstream Close Forced:          0
        Upstream Close Next:            0
        Upstream Close Handshake:       0
        Downstream Close Attempt:       0
        Downstream Close Forced:        0
        Downstream Close Next:          0
        Inbound discard empty buf:      0
        Empty downstream buf:   0
        Encrypt call:           0
        Encrypt call error:     0
        Encrypt handoff:        0
        Encrypt CB success:     0
        Encrypt CB fail:        0
        Flowed Off:             0
        Stats Last State:       0x0  (UNKWN )
        Pending crypto cmds:    0
        Socket Last State:      0x6000 (UNKWN )
        Socket Read State:      0xf0 (read header)
        Handle Read State:      0xf0 (read header)
        References:             NO Session
        In Rekey:               0x0
        Flags:                  0x0
        Header Len:             5
        Record Type:            0x0
        Record Len:             0
        Queued Blocks:          0
        Queued Bytes:           0
0) TM Module
   Mod handle: 0x0000000000xxxxxx
   Rx:  0/1  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
   Tx:  0/1  ( 0 queued), Flow-Ctrl:      0,  Tot:      0
        Transp Flow-Ctrl Rx: 0
        TCP handle: 0x0000xxxxxxxxxxxx, Interface inside (0x2)
        Connection state is LISTEN
        Local host: 0.0.0.0, Local port: 2444
        Foreign host: 0.0.0.0, Foreign port: 0
        Client host: 0.0.0.0, Client port: 0
        TTL Inbound: 0, TTL Outbound: 255
        Datagrams (MSS: send 536, receive 0):
          Retransmit Queue:     0
          Input Queue:          0
          mis-ordered:          0 (0 bytes)
          Rcvd:                 0
            out of order:       0
            with data:          0
            min ttl drop:       0
            total data bytes:   0
          Sent:                 0
            retransmit:         0
            fastretransmit:     0
            partialack:         0
            Second Congestion:  0
            with data:          0
            total data bytes:   0
```

The following is sample output from the **show asp table socket stats** command.

```
TCP Statistics:
  Rcvd:
     total 14794
     checksum errors 0
     no port 0
  Sent:
     total 0
UDP Statistics:
  Rcvd:
     total 0
     checksum errors 0
  Sent:
     total 0
     copied 0
NP SSL System Stats:
  Handshake Started: 33
  Handshake Complete: 33
  SSL Open: 4
  SSL Close: 117
  SSL Server: 58
  SSL Server Verify: 0
  SSL Client: 0
```

TCP/UDP statistics are packet counters representing the number of packets sent or received that are directed to a service that is running or listening on the ASA, such as Telnet, SSH, or HTTPS. Checksum errors are the number of packets dropped because the calculated packet checksum did not match the checksum value stored in the packet (that is, the packet was corrupted). The NP SSL statistics indicate the number of each type of message received. Most indicate the start and completion of new SSL connections to either the SSL server or SSL client.

Related Commands

Command	Description
show asp table vpn-context	Shows the accelerated security path VPN context tables.

show asp table vpn-context

To debug the accelerated security path VPN context tables, use the **show asp table vpn-context** command in privileged EXEC mode.

show asp table vpn-context [**detail**]

Syntax Description

detail	(Optional) Shows additional detail for the VPN context tables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(4)	The +PRESERVE flag for each context that maintains stateful flows after the tunnel drops was added.
9.0(1)	Support for multiple context mode was added.
9.13(1)	To enhance debug capability, following vpn context counters were added to the output: • **Lock Err** : This counter is incremented when a VPN context lock could not be obtained and indicates the number of times this error is encountered. • **No SA** : This counter increments if VPN context receives a packet to be processed but does not have an active SA associated with it. • **IP Ver Err** : This counter increments when an unknown version of IP packet is received. • **Tun Down** : Indicates that the tunnel associated with the VPN context is deleted or the tunnel handle is invalid.

Usage Guidelines

The **show asp table vpn-context** command shows the VPN context contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table vpn-context** command:

```
ciscoasa# show asp table vpn-context
VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

The following is sample output from the **show asp table vpn-context** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag:

```
ciscoasa(config)# show asp table vpn-context

VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

The following is sample output from the **show asp table vpn-context detail** command:

```
ciscoasa# show asp table vpn-context detail
VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

The following is sample output from the **show asp table vpn-context detail** command when the persistent IPsec tunneled flows feature is enabled, as shown by the PRESERVE flag.:

```
ciscoasa(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54
Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
VPN CTX  = 0x0005B234
Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
Pkts     = 0
Bad Pkts = 0
Lock Err = 0
No SA    = 0
IP Ver Err= 0
Tun Down = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
ciscoasa(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

Related Commands

Command	Description
show asp drop	Shows the accelerated security path counters for dropped packets.

show asp table zone

To debug the accelerated security path zone table, use the **show asp table zone** command in privileged EXEC mode.

show asp table zone [*zone_name*]

Syntax Description

zone_name	(Optional) Identifies the zone name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

The **show asp table zone** command shows the contents of the accelerated security path, which might help you troubleshoot a problem. See the CLI configuration guide for more information about the accelerated security path. These tables are used for debugging purposes only, and the information output is subject to change. Consult Cisco TAC to help you debug your system with this command.

Examples

The following is sample output from the **show asp table zone** command:

```
ciscoasa# show asp table zone
Zone: outside-zone id: 2
 Context: test-ctx
  Zone Member(s) : 2
   outside1       GigabitEthernet0/0
   outside2       GigabitEthernet0/1
```

Related Commands

Command	Description
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.
show zone	Shows zone ID, context, security level, and members.

show attribute

To display information related to VM attribute agents and bindings, use the **show attribute** command in EXEC mode.

show attribute [**host-map** [**/all**] **| object-map** [**/all**] **| source-group** *agent-name*]

Syntax Description

host-map	Displays current bindings of virtual machine IP addresses to attributes. Include /all to see binding for all attributes. For example, enter the following: `show attribute host-map /all`
object-map	Displays current bindings of virtual machine IP addresses to attributes. Include /all to see binding for all attributes. For example, enter the following: `show attribute host-map /all`
source-group	Displays the configuration and state of one or more attribute agents. For example, enter the following: `show attribute source-groups` *agent-name*

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
EXEC mode	• Yes	• Yes	• Yes	—	—

Examples

The following is sample output from the **show attribute** commands:

```
ciscoasa# show attribute host-map /all
IP Address-Attribute Bindings Information
        Source/Attribute                        Value
=======================================================================
VMAgent.custom.role                          'Developer'
     169.254.107.176
     169.254.59.151
     10.15.28.34
     10.15.28.32
     10.15.28.31
     10.15.28.33
VMAgent.custom.role                          'Build Machine'
```

```
     10.15.27.133
     10.15.27.135
     10.15.27.134
ciscoasa# show attribute object-map /all
Network Object-Attribute Bindings Information
Object
        Source/Attribute                        Value
=======================================================================
dev
    VMAgent.custom.role                         'Developer'
build
    VMAgent.custom.role                         'Build Machine'
ciscoasa# show attribute source-group
Attribute agent VMAgent
   Agent type: ESXi
   Agent state: Active
   Connection state: Connected
   Host Address: 10.122.202.217
   Retry interval: 30 seconds
   Retry count: 3
   Attributes being monitored:
       'custom.role ' (2)
```

show auto-update

To see the Auto Update Server status, use the **show auto-update** command in privileged EXEC mode.

show auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added..

Usage Guidelines

Use this command to view Auto Update Server status.

Examples

The following is sample output from the **show auto-update** command:

```
ciscoasa(config)# show auto-update
Poll period: 720 minutes, retry count: 0, retry period: 5 minutes
Timeout: none
Device ID: host name [ciscoasa]
```

Related Commands

auto-update device-id	Sets the ASA device ID for use with an Auto Update Server.
auto-update poll-period	Sets how often the ASA checks for updates from an Auto Update Server.
auto-update server	Identifies the Auto Update Server.
auto-update timeout	Stops traffic from passing through the ASA if the Auto Update Server is not contacted within the timeout period.
clear configure auto-update	Clears the Auto Update Server configuration.
show running-config auto-update	Shows the Auto Update Server configuration.

show b – show cq

show backup-package

To display back-up package status and summary information on the Cisco ISA 3000, use the **show backup-package** command in privileged EXEC or global configuration mode.

show backup-package { **status** { **backup | restore** } **| summary** }

Note This command applies only to the Cisco ISA 3000 appliance.

Syntax Description

backup | restore	Specifies the type of **status** information to be displayed.
status	Displays mode, location, passphrase, and most-recent time information for either back-up or restore operations.
summary	Displays status information for both back-up and restore operations.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

The **show backup-package** commands are also available in global configuration mode.

Examples

The following example shows backup-package summary statistics:

```
ciscoasa# show backup-package summary
 backup mode       : auto
 backup location   : disk3:
 backup passphrase: cisco
 last backup time : Mar 23 2014 22:05:52
 restore mode       : auto
 restore location   : disk3:
```

```
restore passphrase: cisco
Last restore time : Mar 24 2014 05:07:32
```

show bfd drops

To display the numbered of dropped packets in BFD, use the show bfd drops command in global configuration mode.

show bfd drops

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example displays the BFD dropped packets.

```
ciscoasa# show bfd drops
BFD Drop Statistics
                         IPV4 IPV6 IPV4-M IPV6-M
Invalid TTL              0    0    0      0
BFD Not Configured       0    0    0      0
No BFD Adjacency         0    0    0      0
Invalid Header Bits      0    0    0      0
Invalid Discriminator    0    0    0      0
Session AdminDown        0    0    0      0
Authen invalid BFD ver   0    0    0      0
Authen invalid len       0    0    0      0
Authen invalid seq       0    0    0      0
Authen failed            0    0    0      0
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.

Command	Description
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

show bfd map

To display the configured BFD maps, use the show bfd map command in global configuration mode.

show bfd map

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Examples

The following example displays the BFD maps.

```
ciscoasa# show bfd map
Destination: 40.40.40.2/24
 Source: 50.50.50.2/24
 Template: mh
 Authentication(Type): sha-1
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.

Command	Description
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.
show bfd summary	Displays summary information for BFD.

show bfd neighbors

To display a line-by-line listing of existing BFD adjacencies, use the show bfd neighbors command in global configuration mode.

show bfd neighbors [**client** { **bgp** } **| details | interface** *interface-name* **| ipv4** *ip-address* **| ipv6** *ipv6-address* **| multihop-ipv4** *ip-address* **| multihop-ipv6** *ipv6-address*]

Syntax Description

client	(Optional) Displays the neighbors of a specific client.
bgp	(Optional) Displays a BGP client.
details	(Optional) Displays all BFD protocol parameters and timers for each neighbor.
interface interface-name	(Optional) Displays neighbors at the specified interface.
ipv4 ip-address	(Optional) Displays specified single-hop IP neighbors.
ipv6 ipv6-address	(Optional) Displays specified single-hop IPv6 neighbors.
multihop-ipv4 ip-address	(Optional) Displays specified multi-hop IP neighbors.
multihop-ipv6 ipv6-address	(Optional) Displays specified multi-hop IPv6 neighbors.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to troubleshoot BFD issues.

Examples

The following example displays the BFD neighbors.

```
ciscoasa# show bfd neighbors
OurAddr     NeighAddr    LD/RD  RH     Holdown(mult)     State Int
172.16.10.1 172.16.10.2  1/6    1      260 (3 )          Up    Fa0/1
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd summary	Displays summary information for BFD.

show bfd summary

To display summary information for BFD, use the show bfd summary command in global configuration mode.

show bfd summary [**client** | **host** | **session**]

Syntax Description

client	(Optional) Displays the BFD summary for clients.
host	(Optional) Displays the BFD summary for sessions.
session	(Optional) Displays the BFD summary for protocols.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to display summary information about BFD, BFD clients, or BFD sessions. When a BFD client launches a session with a peer, BFD sends periodic BFD control packets to the peer. Information about the following states of a session are included in the output of this command:

- Up—When another BFD interface acknowledges the BFD control packets, the session moves into an Up state.
- Down—The session and the data path are declared down if a data path failure occurs and BFD does not receive a control packet within the configured amount of time. When a session is down, BFD notifies the BFD client so that the client can perform necessary actions to reroute the traffic.

Examples

The following example displays the BFD summaries.

```
ciscoasa# show bfd summary

         Session         Up       Down
Total    1               1        0
ciscoasa# show bfd summary session
Protocol                  Session     Up  Down
IPV4                      1     1     0
```

```
Total                     1     1     0
ciscoasa# show bfd summary client
Client                   Session      Up     Down
BGP                      1       1    0
EIGRP                    1       1    0
Total                    2       2    0
```

Related Commands

Command	Description
authentication	Configures authentication in a BFD template for single-hop and multi-hop sessions.
bfd echo	Enables BFD echo mode on the interface,
bfd interval	Configures the baseline BFD parameters on the interface.
bfd map	Configures a BFD map that associates addresses with multi-hop templates.
bfd slow-timers	Configures the BFD slow timers value.
bfd template	Binds a single-hop BFD template to an interface.
bfd-template single-hop | multi-hop	Configures the BFD template and enters BFD configuration mode.
clear bfd counters	Clears the BFD counters.
echo	Configures echo in the BFD single-hop template.
neighbor	Configures BFD support for BGP so that BGP is registered to receive forwarding path detection failure messages from BFD.
show bfd drops	Displays the numbered of dropped packets in BFD.
show bfd map	Displays the configured BFD maps.
show bfd neighbors	Displays a line-by-line listing of existing BFD adjacencies.

show bgp

To display entries in the Border Gateway Protocol (BGP) routing table, use the show bgp command in user EXEC or privileged EXEC mode.

show bgp [*ip-address* [*mask* [**longer-prefixes** [**injected**] **| shorter-prefixes** [*length*] **| bestpath | multipaths | subnets**] **| bestpath | multipaths**] **| all | prefix-list name | pending-prefixes | route-map** *name*]]

Syntax Description

ip-address	(Optional) Specifies the AS path access list name..
mask	(Optional) Mask to filter or match hosts that are part of the specified network.
longer-prefixes	(Optional) Displays the specified route and all more specific routes.
injected	(Optional) Displays more specific prefixes injected into the BGP routing table.
shorter-prefixes	(Optional) Displays the specified route and all less specific routes.
length	(Optional) The prefix length. The value for this argument is a number from 0 to 32.
bestpath	(Optional) Displays the bestpath for this prefix
multipaths	(Optional) Displays multipaths for this prefix.
subnets	(Optional) Displays the subnet routes for the specified prefix.
all	(Optional) Displays all address family information in the BGP routing table.
prefix-list name	(Optional) Filters the output based on the specified prefix list.
pending-prefixes	(Optional) Displays prefixes that are pending deletion from the BGP routing table.
route-map name	(Optional) Filters the output based on the specified route map.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

The show bgp command is used to display the contents of the BGP routing table. The output can be filtered to display entries for a specific prefix, prefix length, and prefixes injected through a prefix list, route map, or conditional advertisement.

In Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, and later releases, the Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command followed by the clear bgp * command to perform a hard reset of all current BGP sessions.

Examples

The following sample output shows the BGP routing table:

```
Router# show bgp
BGP table version is 22, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.1/32      0.0.0.0                  0         32768 i
*>i10.2.2.2/32      172.16.1.2               0    100      0 i
*bi10.9.9.9/32      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
* i172.16.1.0/24    172.16.1.2               0    100      0 i
*>                  0.0.0.0                  0         32768 i
*> 192.168.1.0      0.0.0.0                  0         32768 i
*>i192.168.3.0      172.16.1.2               0    100      0 i
*bi192.168.9.0      192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
*bi192.168.13.0     192.168.3.2              0    100      0 10 10 i
*>                  192.168.1.2                            0 10 10 i
```

Table 5: show bgp Fields shows each field description.

Table 5: show bgp Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry is a RIB-failure. • S—The table entry is stale. • m—The table entry has multipath to use for that network. • b—The table entry has backup path to use for that network. • x—The table entry has best external route to use for the network.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
(stale)	Indicates that the following path for the specified autonomous system is marked as "stale" during a graceful restart process.

Examples

show bgp (4-Byte Autonomous System Numbers): Example

The following sample output shows the BGP routing table with 4-byte autonomous system numbers, 65536 and 65550, shown under the Path field. This example requires Cisco IOS Release 12.0(32)SY8, 12.0(33)S3, 12.2(33)SRE, 12.2(33)XNE, 12.2(33)SXI1, Cisco IOS XE Release 2.4, or a later release.

```
RouterB# show bgp
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 65536  i
*> 10.2.2.0/24      192.168.3.2              0             0 65550  i
*> 172.17.1.0/24    0.0.0.0                  0         32768 i
```

show bgp ip-address: Example

The following sample output displays information about the 192.168.1.0 entry in the BGP routing table:

```
Router# show bgp 192.168.1.0
BGP routing table entry for 192.168.1.0/24, version 22
Paths: (2 available, best #2, table default)
  Additional-path
  Advertised to update-groups:
     3
  10 10
    192.168.3.2 from 172.16.1.2 (10.2.2.2)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
  10 10
    192.168.1.2 from 192.168.1.2 (10.3.3.3)
      Origin IGP, localpref 100, valid, external, best , recursive-via-connected
```

The following sample output displays information about the 10.3.3.3 255.255.255.255 entry in the BGP routing table:

```
Router# show bgp 10.3.3.3 255.255.255.255
BGP routing table entry for 10.3.3.3/32, version 35
Paths: (3 available, best #2, table default)
Multipath: eBGP
Flag: 0x860
  Advertised to update-groups:
     1
  200
    10.71.8.165 from 10.71.8.165 (192.168.0.102)
      Origin incomplete, localpref 100, valid, external, backup/repair
      Only allowed to recurse through connected route
  200
    10.71.11.165 from 10.71.11.165 (192.168.0.102)
      Origin incomplete, localpref 100, weight 100, valid, external, best
      Only allowed to recurse through connected route
  200
    10.71.10.165 from 10.71.10.165 (192.168.0.104)
      Origin incomplete, localpref 100, valid, external,
      Only allowed to recurse through connected route
```

Table 6: show bgp (4 byte autonomous system numbers) Fields shows each field description.

Table 6: show bgp (4 byte autonomous system numbers) Fields

Field	Description
BGP routing table entry fo	IP address or network number of the routing table entry.
version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	The number of available paths, and the number of installed best paths. This line displays “Default-IP-Routing-Table” when the best path is installed in the IP routing table.
Multipath	This field is displayed when multipath loadsharing is enabled. This field will indicate if the multipaths are iBGP or eBGP.
Advertised to update-groups	The number of each update group for which advertisements are processed.
Origin	Origin of the entry. The origin can be IGP, EGP, or incomplete. This line displays the configured metric (0 if no metric is configured), the local preference value (100 is default), and the status and type of route (internal, external, multipath, best).
Extended Community	This field is displayed if the route carries an extended community attribute. The attribute code is displayed on this line. Information about the extended community is displayed on a subsequent line.

Examples

show bgp all: Example

The following is sample output from the show bgp command entered with the all keyword. Information about all configured address families is displayed.

```
Router# show bgp all
For address family: IPv4 Unicast   *****
BGP table version is 27, local router ID is 10.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      0.0.0.0                  0         32768 ?
*> 10.13.13.0/24    0.0.0.0                  0         32768 ?
*> 10.15.15.0/24    0.0.0.0                  0         32768 ?
*>i10.18.18.0/24    172.16.14.105         1388  91351      0 100 e
*>i10.100.0.0/16    172.16.14.107          262    272      0 1 2 3 i
*>i10.100.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.101.0.0/16    172.16.14.105         1388  91351      0 100 e
*>i10.103.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.104.0.0/16    172.16.14.101         1388    173    173 100 e
*>i10.100.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*>i10.101.0.0/16    172.16.14.106         2219  20889      0 53285 33299 51178 47751 e
*  10.100.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*  10.101.0.0/16    172.16.14.109         2309             0 200 300 e
*>                  172.16.14.108         1388             0 100 e
*> 10.102.0.0/16    172.16.14.108         1388             0 100 e
*> 172.16.14.0/24   0.0.0.0                  0         32768 ?
*> 192.168.5.0      0.0.0.0                  0         32768 ?
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
*> 10.80.0.0/16     172.16.14.108         1388             0 50 e
```

show bgp longer-prefixes: Example

The following is sample output from the show bgp command entered with the longer-prefixes keyword:

```
Router# show bgp 10.92.0.0 255.255.0.0 longer-prefixes
BGP table version is 1738, local router ID is 192.168.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 10.92.0.0         10.92.72.30        8896         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.1.0         10.92.72.30        8796         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.11.0        10.92.72.30       42482         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.14.0        10.92.72.30        8796         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.15.0        10.92.72.30        8696         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.16.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.17.0        10.92.72.30        1400         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.18.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
*> 10.92.19.0        10.92.72.30        8876         32768 ?
*                    10.92.72.30                         0 109 108 ?
```

show bgp shorter-prefixes: Example

The following is sample output from the show bgp command entered with the shorter-prefixes keyword. An 8-bit prefix length is specified.

```
Router# show bgp 172.16.0.0/16 shorter-prefixes 8
*> 172.16.0.0         10.0.0.2                              0 ?
*                     10.0.0.2                 0            0 200 ?
```

show bgp prefix-list: Example

The following is sample output from the show bgp command entered with the prefix-list keyword:

```
Router# show bgp prefix-list ROUTE
BGP table version is 39, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                              0 ?
*                   10.0.0.2                 0            0 200 ?
```

show bgp route-map: Example

The following is sample output from the show bgp command entered with the route-map keyword:

```
Router# show bgp route-map LEARNED_PATH
BGP table version is 40, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
```

```
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 192.168.1.0      10.0.0.2                               0 ?
*                   10.0.0.2                 0             0 200 ?
```

show bgp all community

To display routes for all address families belonging to a particular Border Gateway Protocol (BGP) community, use the show bgp all community command in user EXEC or privileged EXEC configuration mode.

show bgp all community [*community-number....* [*community-number*]] [**local-as**] [**no-advertise**] [**no-export**] [**exact-match**]

Syntax Description

community-number.	(Optional) Displays the routes pertaining to the community numbers specified. You can specify multiple community numbers. The range is from 1 to 4294967295 or AA:NN (autonomous system:community number, which is a 2-byte number).
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).
exact-match	(Optional) Displays only routes that match exactly with the BGP community list specified. **Note** The availability of keywords in the command depends on the command mode. The exact-match keyword is not available in user EXEC mode.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

User can enter the local-as, no-advertise and no-export keywords in any order. When using the bgp all community command, be sure to enter the numerical communities before the well-known communities.

.For example, the following string is not valid:

```
ciscoasa# show bgp all community local-as 111:12345
```

Use the following string instead:

```
ciscoasa# show bgp all community 111:12345 local-as
```

Examples

The following is sample output from the show bgp all community command, specifying communities of 1, 2345, and 6789012:

```
ciscoasa# show bgp all community 1 2345 6789012 no-advertise local-as no-export exact-match
For address family: IPv4 Unicast
BGP table version is 5, local router ID is 30.0.0.5
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network     Next Hop            Metric LocPrf Weight  Path
*> 10.0.3.0/24       10.0.0.4                             0 4 3 ?
*> 10.1.0.0/16       10.0.0.4                 0           0 4 ?
*> 10.12.34.0/24     10.0.0.6                 0           0 6 ?
```

Table 30: show blocks Fields shows each field description.

Table 7: show bgp all community Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes
local router ID	The router ID of the router on which the BGP communities are set to display. A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. d—The table entry is dampened.h—The table entry is history.*—The table entry is valid.>—The table entry is the best entry to use for that network.i—The table entry was learned via an internal BGP session.
Origin codes	Indicates the origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from the Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from the Exterior Gateway Protocol (EGP).?—Origin of the path is not clear. Usually, this is a route that is redistributed into BGP from an IGP.
Network	The network address and network mask of a network entity. The type of address depends on the address family.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. The type of address depends on the address family
Metric	The value of the inter autonomous system metric. This field is not used frequently.

Field	Description
LocPrf	Local preference value as set with the set local-preference command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

show bgp all neighbors

To display information about Border Gateway Protocol (BGP) connections to neighbors of all address families, use the show bgp all neighbors command in user EXEC or privileged EXEC mode.

show bgp all neighbors [*ip-address*] [**advertised-routes | paths** [*reg-exp*] **| policy** [**detail**] **| received prefix-filter | received-routes | routes**]

Syntax Description

ip-address	(Optional) IP address of a neighbor. If this argument is omitted, information about all neighbors is displayed.
advertised-routes	Optional) Displays all routes that have been advertised to neighbors.
paths reg-exp	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, Access Control Lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.

Command Default

The output of this command displays information for all neighbors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

Use the show bgp all neighbors command to display BGP and TCP connection information for neighbor sessions specific to address families such as IPv4.

Examples

The following example shows output of the show bgp all neighbors command:

```
ciscoasa# show bgp all neighbors
For address family: IPv4 Unicast
BGP neighbor is 172.16.232.53, remote AS 100, external link
 Member of peer-group internal for session parameters
  BGP version 4, remote router ID 172.16.232.53
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        11
  Default minimum time between advertisement runs is 5 seconds
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent:4445 (retransmit: 5), with data: 4445, total data bytes;244128
```

Table 8: show bgp all neighbor Fields shows each field description.

Table 8: show bgp all neighbor Fields

Field	Description
For address family	Address family to which the following fields refer.
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
external link	External Border Gateway Protocol (eBGP) peerP.

Field	Description
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	State of this BGP connection
up for	Time, in hh:mm:ss, that the underlying TCP connection has been in existence.
Last read	Time, in hh:mm:ss, since BGP last received a message from this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Rcvd	Total number of received messages.
Opens	Number of open messages sent and received.
Notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time, in hh:mm:ss, since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be...	Indicates that the BGP Time-to-live (TTL) security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.

Field	Description
Local host, Local	IP address of the local BGP speaker and the port number.
Foreign host, Foreign port	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer.
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna:	Last transmission sequence number that has not been acknowledged
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote host.
irs:	Initial packet receives sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.

Field	Description
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
with data	Number of update packets received with data.
total data bytes	Total amount of data sent, in bytes.

show bgp cidr-only

To display routes with classless inter domain routing (CIDR), use the show bgp cidr-only command in EXEC mode.

show bgp cidr-only

Syntax Description

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the show bgp cidr-only command:

```
 ciscoasa# show bgp cidr-only

BGP table version is 220, local router ID is 172.16.73.131
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*> 192.168.0.0/8    172.16.72.24                       0 1878 ?
*> 172.16.0.0/16    172.16.72.30                       0 108 ?
```

Table 9: show bgp cidr-only Fieldsshows each field description.

Table 9: show bgp cidr-only Fields

Field	Description
BGP table version is 220	Internal version number of the table. This number is incremented whenever the table changes..
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP..

show bgp community

To display routes that belong to specified BGP communities, use the show bgp community command in EXEC mode.

show bgp community *community-number* [**exact**]

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the show bgp community command in privileged EXEC mode:

```
ciscoasa# show bgp community 111:12345 local-as
 BGP table version is 10, local router ID is 224.0.0.10
 Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
 Origin codes: i - IGP, e - EGP, ? - incomplete

    Network          Next Hop          Metric LocPrf Weight Path
 *> 172.16.2.2/32    10.43.222.2            0             0 222 ?
 *> 10.0.0.0         10.43.222.2            0             0 222 ?
 *> 10.43.0.0        10.43.222.2            0             0 222 ?
 *> 10.43.44.44/32   10.43.222.2            0             0 222 ?
 *  10.43.222.0/24   10.43.222.2            0             0 222 i
 *> 172.17.240.0/21  10.43.222.2            0             0 222 ?
 *> 192.168.212.0    10.43.222.2            0             0 222 i
 *> 172.31.1.0       10.43.222.2            0             0 222 ?
```

Table 10: show bgp community Fieldsshows each field description.

Table 10: show bgp community Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp community-list

To display routes that are permitted by the Border Gateway Protocol (BGP) community list, use the show bgp community-list command in user or privileged EXEC mode.

show bgp community-list { *community-list-number* | *community-list-name* [**exact-match**] }

Syntax Description

community-list-number	A standard or expanded community list number in the range from 1 to 500.
community-list-name	Community list name. The community list name can be standard or expanded.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

This command requires you to specify an argument when used. The exact-match keyword is optional.

Examples

The following is sample output of the show bgp community-list command in privileged EXEC mode:

```
ciscoasa# show bgp community-list 20
BGP table version is 716977, local router ID is 192.168.32.1
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
* i10.3.0.0         10.0.22.1             0    100      0 1800 1239 ?
*>i                 10.0.16.1             0    100      0 1800 1239 ?
* i10.6.0.0         10.0.22.1             0    100      0 1800 690 568 ?
*>i                 10.0.16.1             0    100      0 1800 690 568 ?
* i10.7.0.0         10.0.22.1             0    100      0 1800 701 35 ?
*>i                 10.0.16.1             0    100      0 1800 701 35 ?
*                   10.92.72.24                         0 1878 704 701 35 ?
* i10.8.0.0         10.0.22.1             0    100      0 1800 690 560 ?
*>i                 10.0.16.1             0    100      0 1800 690 560 ?
*                   10.92.72.24                         0 1878 704 701 560 ?
* i10.13.0.0        10.0.22.1             0    100      0 1800 690 200 ?
*>i                 10.0.16.1             0    100      0 1800 690 200 ?
*                   10.92.72.24                         0 1878 704 701 200 ?
* i10.15.0.0        10.0.22.1           0    100      0 1800 174 ?
*>i                 10.0.16.1           0    100      0 1800 174 ?
* i10.16.0.0        10.0.22.1           0    100      0 1800 701 i
*>i                 10.0.16.1           0    100      0 1800 701 i
*                   10.92.72.24                       0 1878 704 701 i
```

Table 11: show bgp community-list Fields shows each field description.

Table 11: show bgp community-list Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP..

show bgp filter-list

To display routes that conform to a specified filter list, use the show bgp filter-list command in EXEC mode.

show bgp filter-list *access-list-name*

Syntax Description

access-list-name	Name of an autonomous system path access list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output of the show bgp filter-list command in privileged EXEC mode:

```
ciscoasa# show bgp filter-list filter-list-acl
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                       0 109 108 ?
*  172.16.1.0       172.16.72.30                       0 109 108 ?
*  172.16.11.0      172.16.72.30                       0 109 108 ?
*  172.16.14.0      172.16.72.30                       0 109 108 ?
*  172.16.15.0      172.16.72.30                       0 109 108 ?
*  172.16.16.0      172.16.72.30                       0 109 108 ?
*  172.16.17.0      172.16.72.30                       0 109 108 ?
*  172.16.18.0      172.16.72.30                       0 109 108 ?
*  172.16.19.0      172.16.72.30                       0 109 108 ?
*  172.16.24.0      172.16.72.30                       0 109 108 ?
*  172.16.29.0      172.16.72.30                       0 109 108 ?
*  172.16.30.0      172.16.72.30                       0 109 108 ?
*  172.16.33.0      172.16.72.30                       0 109 108 ?
*  172.16.35.0      172.16.72.30                       0 109 108 ?
*  172.16.36.0      172.16.72.30                       0 109 108 ?
*  172.16.37.0      172.16.72.30                       0 109 108 ?
*  172.16.38.0      172.16.72.30                       0 109 108 ?
*  172.16.39.0      172.16.72.30                       0 109 108 ?
```

Table 12: show bgp filter-list Fields shows each field description.

Table 12: show bgp filter-list Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP..

show bgp injected-paths

To display all the injected paths in the Border Gateway Protocol (BGP) routing table, use the show bgp injected-paths command in user or privileged EXEC mode.

show bgp injected-paths

Syntax Description

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the show bgp injected-paths command in EXEC mode:

```
ciscoasa# show bgp injected-paths
BGP table version is 11, local router ID is 10.0.0.1
Status codes:s suppressed, d damped, h history, * valid, > best, i -
internal
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 172.16.0.0       10.0.0.2                               0 ?
*> 172.17.0.0/16    10.0.0.2                               0 ?
```

Table 13: show bgp injected-path Fields shows each field description.

Table 13: show bgp injected-path Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv4

To display entries in the IP version 4 (IPv4) Border Gateway Protocol (BGP) routing table, use the show bgp ipv4 command in privileged EXEC mode.

show bgp ipv4

Syntax Description

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the show bgp ipv4 unicast command:

```
ciscoasa# show bgp ipv4 unicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

The following is sample output from the show bgp ipv4 multicast command:

```
Router# show bgp ipv4 multicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

show bgp ipv4 shows each field description.

Table 14: show bgp ipv4 Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP..

show bgp ipv6

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the show bgp ipv6 command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast [*ipv6-prefix/prefix-length*] [**longer-prefixes**] [**labels**]

Syntax Description

unicast	*Specifies IPv6 unicast address prefixes.*
ipv6-prefix	(Optional) IPv6 network number, entered to display a particular network in the IPv6 BGP routing table. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/prefix-length	(Optional) The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer-prefixes	(Optional) Displays the route and more specific routes.
labels	(Optional) Displays the policies applied to this neighbor per address family.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context	
	Routed	Transparent	Single	Multiple
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The following is sample output from the show bgp ipv6 command:

```
ciscoasa# show bgp ipv6 unicast
BGP table version is 12612, local router ID is 172.16.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1             0            0  300 i
*> 10.10.20.0/24   172.16.10.1             0            0  300 i
*  10.20.10.0/24   172.16.10.1             0            0  300 i
```

The following is sample output from the show bgp ipv4 multicast command:

```
Router# show bgp ipv4 multicast
 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network             Next Hop            Metric LocPrf Weight Path
*                    3FFE:C00:E:C::2                        0 3748 4697 1752 i
*                    3FFE:1100:0:CC00::1
                                                            0 1849 1273 1752 i
*  2001:618:3::/48   3FFE:C00:E:4::2          1             0 4554 1849 65002 i
*>                   3FFE:1100:0:CC00::1
                                                            0 1849 65002 i
*  2001:620::/35     2001:0DB8:0:F004::1
                                                            0 3320 1275 559 i
*                    3FFE:C00:E:9::2                        0 1251 1930 559 i
*                    3FFE:3600::A                           0 3462 10566 1930 559 i
*                    3FFE:700:20:1::11
                                                            0 293 1275 559 i
*                    3FFE:C00:E:4::2          1             0 4554 1849 1273 559 i
*                    3FFE:C00:E:B::2                        0 237 3748 1275 559 i
```

Table 14: show bgp ipv4 Fields shows each field description.

Table 15: show bgp ipv6 Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

The following is sample output from the show bgp ipv6 command, showing information for prefix 3FFE:500::/24:

```
ciscoasa# show bgp ipv6 unicast 3FFE:500::/24
BGP routing table entry for 3FFE:500::/24, version 19421
Paths: (6 available, best #1)
  293 3425 2500
    3FFE:700:20:1::11 from 3FFE:700:20:1::11 (192.168.2.27)
      Origin IGP, localpref 100, valid, external, best
  4554 293 3425 2500
    3FFE:C00:E:4::2 from 3FFE:C00:E:4::2 (192.168.1.1)
      Origin IGP, metric 1, localpref 100, valid, external
  33 293 3425 2500
    3FFE:C00:E:5::2 from 3FFE:C00:E:5::2 (209.165.18.254)
      Origin IGP, localpref 100, valid, external
  6175 7580 2500
    3FFE:C00:E:1::2 from 3FFE:C00:E:1::2 (209.165.223.204)
      Origin IGP, localpref 100, valid, external
1849 4697 2500, (suppressed due to dampening)
    3FFE:1100:0:CC00::1 from 3FFE:1100:0:CC00::1 (172.31.38.102)
      Origin IGP, localpref 100, valid, external
237 10566 4697 2500
    3FFE:C00:E:B::2 from 3FFE:C00:E:B::2 (172.31.0.3)
      Origin IGP, localpref 100, valid, external
ciscoasa# show bgp ipv6 unicast
BGP table version is 28, local router ID is 172.10.10.1
Status codes:s suppressed, h history, * valid, > best, i -
internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i4004::/64        ::FFFF:172.11.11.1
                                             0    100      0 ?
* i                 ::FFFF:172.30.30.1
                                             0    100      0 ?
```

show bgp ipv6 community

To display entries in the IPv6 Border Gateway Protocol (BGP) routing table, use the show bgp ipv6community command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast community [*community-number*] [**exact-match**] [**local-as | no-advertise | no-export**]

Syntax Description

unicast	*Specifies IPv6 unicast address prefixes.*
community-number	(Optional) Valid value is a community number in the range from 1 to 4294967295 or AA:NN (autonomous system-community number:2-byte number).
exact-match	(Optional) Displays only routes that have an exact match.
local-as	(Optional) Displays only routes that are not sent outside of the local autonomous system (well-known community).
no-advertise	(Optional) Displays only routes that are not advertised to any peer (well-known community).
no-export	(Optional) Displays only routes that are not exported outside of the local autonomous system (well-known community).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The show bgp ipv6 community command provides output similar to the show ip bgp community command, except it is IPv6-specific.

Communities are set with the set community route-map configuration command. You must enter the numerical communities before the well-known communities. For example, the following string is not valid:

```
ciscoasa# show ipv6 bgp unicast community local-as 111:12345
```

Use following strings instead:

```
ciscoasa# show ipv6 bgp unicast community 111:12345 local-as
```

Examples

The following is sample output from the show bgp ipv6 community command:

```
BGP table version is 69, local router ID is 10.2.64.5
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
       Network              Next Hop              Metric LocPrf Weight Path
*> 2001:0DB8:0:1::1/64      ::                                       0 32768 i
*> 2001:0DB8:0:1:1::/80     ::                                       0 32768 ?
*> 2001:0DB8:0:2::/64       2001:0DB8:0:3::2                            0 2 i
*> 2001:0DB8:0:2:1::/80     2001:0DB8:0:3::2                            0 2 ?
* 2001:0DB8:0:3::1/64       2001:0DB8:0:3::2                            0 2 ?
*>                       ::                                       0 32768 ?
*> 2001:0DB8:0:4::/64       2001:0DB8:0:3::2                            0 2 ?
*> 2001:0DB8:0:5::1/64      ::                                       0 32768 ?
*> 2001:0DB8:0:6::/64       2000:0:0:3::2                            0 2 3 i
*> 2010::/64                ::                                       0 32768 ?
*> 2020::/64                ::                                       0 32768 ?
*> 2030::/64                ::                                       0 32768 ?
*> 2040::/64                ::                                       0 32768 ?
*> 2050::/64                ::                                       0 32768 ?
```

Table 16: show bgp ipv6 community fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.

Field	Description
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 community-list

To display routes that are permitted by the IPv6 Border Gateway Protocol (BGP) community list, use the show bgp ipv6 community-list command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast community-list { *number* | *name* } [**exact-match**]

Syntax Description

unicast	*Specifies IPv6 unicast address prefixes.*
number	Community list number in the range from 1 to 199.
name	Community list name.
exact-match	(Optional) Displays only routes that have an exact match.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The show bgp ipv6 unicast community-list command provide output similar to the show ip bgp community-list command, except they are IPv6-specific.

Examples

The following is sample output of the show bgp ipv6 community-list command for community list number 3:

```
ciscoasa# show bgp ipv6 unicast community-list 3
BGP table version is 14, local router ID is 10.2.64.6
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network                 Next Hop            Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64       2001:0DB8:0:3::1                          0 1 i
*> 2001:0DB8:0:1:1::/80     2001:0DB8:0:3::1                          0 1 i
*> 2001:0DB8:0:2::1/64      ::                                     0 32768 i
*> 2001:0DB8:0:2:1::/80     ::                                     0 32768 ?
* 2001:0DB8:0:3::2/64      2001:0DB8:0:3::1                          0 1 ?
*>                        ::                                    0 32768 ?
*> 2001:0DB8:0:4::2/64      ::                                     0 32768 ?
*> 2001:0DB8:0:5::/64       2001:0DB8:0:3::1                     0 1 ?
*> 2010::/64                2001:0DB8:0:3::1                     0 1 ?
*> 2020::/64                2001:0DB8:0:3::1                     0 1 ?
*> 2030::/64                2001:0DB8:0:3::1                     0 1 ?
*> 2040::/64                2001:0DB8:0:3::1                     0 1 ?
*> 2050::/64                2001:0DB8:0:3::1                     0 1 ?
```

Table below describes the significant fields shown in the display.

Table 17: show bgp ipv6 community-list fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 filter-list

To display routes that conform to a specified IPv6 filter list, use the show bgp ipv6 filter-list command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast filter-list *access-list-number*

Syntax Description

unicast	*Specifies IPv6 unicast address prefixes.*
>*access-list-number*	Number of an IPv6 autonomous system path access list. It can be a number from 1 to 199.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The show bgp ipv6 filter-list command provides output similar to the show ip bgp filter-list command, except that it is IPv6-specific.

Examples:

The following is sample output from the show bgp ipv6 filter-list command for IPv6 autonomous system path access list number 1:

```
ciscoasa# show bgp ipv6 unicast filter-list 1
BGP table version is 26, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
    Network              Next Hop                          Metric LocPrf Weight Path
*> 2001:0DB8:0:1::/64        2001:0DB8:0:4::2                        0 2 1 i
*> 2001:0DB8:0:1:1::/80      2001:0DB8:0:4::2                        0 2 1 i
*> 2001:0DB8:0:2:1::/80      2001:0DB8:0:4::2                        0 2 ?
*> 2001:0DB8:0:3::/64        2001:0DB8:0:4::2                        0 2 ?
*> 2001:0DB8:0:4::/64        ::                                        32768  ?
*                            2001:0DB8:0:4::2                        0 2 ?
*> 2001:0DB8:0:5::/64        ::                                        32768  ?
*                            2001:0DB8:0:4::2                        0 2 1 ?
*> 2001:0DB8:0:6::1/64       ::                                        32768  i
*> 2030::/64                 2001:0DB8:0:4::2                        0 1
*> 2040::/64              2001:0DB8:0:4::2                        0 2 1 ?
*> 2050::/64              2001:0DB8:0:4::2                        0 2 1 ?
Table below describes the significant fields shown in the display.
```

Table 18: show bgp ipv6 community-list fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.

Field	Description
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 inconsistent-as

To display IPv6 Border Gateway Protocol (BGP) routes with inconsistent originating autonomous systems, use the show bgp ipv6 inconsistent-as command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast inconsistent-as

Syntax Description

unicast	*Specifies IPv6 unicast address prefixes.*

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The show bgp ipv6 unicast inconsistent-as command provide output similar to the show ip bgp inconsistent-as command, except they are IPv6-specific.

Examples

The following is sample output from the show bgp ipv6 inconsistent-as command:

```
ciscoasa# show bgp ipv6 unicast inconsistent-as
BGP table version is 12612, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  3FFE:1300::/24   2001:0DB8:0:F004::1                    0 3320 293 6175 ?
*                   3FFE:C00:E:9::2                        0 1251 4270 10318 ?
*                   3FFE:3600::A                           0 3462 6175 ?
*                   3FFE:700:20:1::11                      0 293 6175 ?Table 19: show bgp
ipv6 community-list fields below describes the significant fields shown in the display.
```

Table 19: show bgp ipv6 community-list fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 neighbors

To display information about IPv6 Border Gateway Protocol (BGP) connections to neighbors, use the **show bgp ipv6 neighbors** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast neighbors [*ipv6-address*] [**received-routes | routes | advertised-routes | paths** *regular-expression*]

Syntax Description

unicast	*Specifies IPv6 unicast address prefixes.*
ipv6-address	(Optional) Address of the IPv6 BGP-speaking neighbor. If you omit this argument, all IPv6 neighbors are displayed. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes received and accepted. This is a subset of the output from the **received-routes** keyword.
advertised-routes	(Optional) Displays all the routes the networking device advertised to the neighbor.
paths *regular-expression*	(Optional) Regular expression used to match the paths received.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This **command was added.**

Examples

The **show bgp ipv6 unicast neighbors** provide output similar to the **show ip bgp neighbors** command, except they are IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6 neighbors** command:

```
ciscoasa# show bgp ipv6 unicast neighbors
BGP neighbor is 3FFE:700:20:1::11,  remote AS 65003, external link
  BGP version 4, remote router ID 192.168.2.27
  BGP state = Established, up for 13:40:17
  Last read 00:00:09, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received
    Address family IPv6 Unicast: advertised and received
  Received 31306 messages, 20 notifications, 0 in queue
  Sent 14298 messages, 1 notifications, 0 in queue
  Default minimum time between advertisement runs is 30 seconds
 For address family: IPv6 Unicast
  BGP table version 21880, neighbor version 21880
  Index 1, Offset 0, Mask 0x2
  Route refresh request: received 0, sent 0
  Community attribute sent to this neighbor
  Outbound path policy configured
  Incoming update prefix filter list is bgp-in
  Outgoing update prefix filter list is aggregate
  Route map for outgoing advertisements is uni-out
  77 accepted prefixes consume 4928 bytes
  Prefix advertised 4303, suppressed 0, withdrawn 1328
  Number of NLRIs in the update sent: max 1, min 0
  1 history paths consume 64 bytes
  Connections established 22; dropped 21
  Last reset 13:47:05, due to BGP Notification sent, hold time expired
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Local host: 3FFE:700:20:1::12, Local port: 55345
Foreign host: 3FFE:700:20:1::11, Foreign port: 179
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x1A0D543C):
Timer          Starts    Wakeups            Next
Retrans          1218          5             0x0
TimeWait            0          0             0x0
AckHold          3327       3051             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 1805423033  snduna: 1805489354  sndnxt: 1805489354     sndwnd:  15531
irs:  821333727  rcvnxt:  821591465  rcvwnd:      15547  delrcvwnd:    837
SRTT: 300 ms, RTTO: 303 ms, RTV: 3 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, nagle
Datagrams (max data segment is 1420 bytes):
Rcvd: 4252 (out of order: 0), with data: 3328, total data bytes: 257737
Sent: 4445 (retransmit: 5), with data: 4445, total data bytes: 244128
```

The table below describes the significant fields shown in the display.

Table 20: show bgp ipv6 community-list fields

Field	Description
BGP neighbor	IP address of the BGP neighbor and its autonomous system number. If the neighbor is in the same autonomous system as the router, then the link between them is internal; otherwise, it is considered external.
remote AS	Autonomous system of the neighbor.

Field	Description
internal link	Indicates that this peer is an interior Border Gateway Protocol (iBGP) peer.
BGP version	BGP version being used to communicate with the remote router; the router ID (an IP address) of the neighbor is also specified.
remote router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
BGP state	Internal state of this BGP connection.
up for	Amount of time that the underlying TCP connection has been in existence.
Last read	Time that BGP last read a message from this neighbor.
hold time	Maximum amount of time that can elapse between messages from the peer.
keepalive interval	Time period between sending keepalive packets, which help ensure that the TCP connection is up.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor.
Route refresh	Indicates that the neighbor supports dynamic soft reset using the route refresh capability.
Address family IPv6 Unicast	Indicates that BGP peers are exchanging IPv6 reachability information.
Received	Number of total BGP messages received from this peer, including keepalives.
notifications	Number of error messages received from the peer .
Sent	Total number of BGP messages that have been sent to this peer, including keepalives.
notifications	Number of error messages the router has sent to this peer.
advertisement runs	Value of the minimum advertisement interval.
For address family	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
neighbor version	Number used by the software to track the prefixes that have been sent and those that must be sent to this neighbor.
Route refresh request	Number of route refresh requests sent and received from this neighbor. .

Field	Description
Community attribute (not shown in sample output)	Appears if the neighbor send-community command is configured for this neighbor. .
Inbound path policy (not shown in sample output)	Indicates whether an inbound filter list or route map is configured.
Outbound path policy (not shown in sample output)	Indicates whether an outbound filter list, route map, or unsuppress map is configured.
bgp-in (not shown in sample output)	Name of the inbound update prefix filter list for the IPv6 unicast address family.
aggregate (not shown in sample output)	Name of the outbound update prefix filter list for the IPv6 unicast address family.
uni-out (not shown in sample output)	Name of the outbound route map for the IPv6 unicast address family.
accepted prefixes	Number of prefixes accepted.
Prefix advertised	Number of prefixes advertised.
suppressed	Number of prefixes suppressed
withdrawn	Number of prefixes withdrawn.
history paths (not shown in sample output)	Number of path entries held to remember history.
Connections established	Number of times the router has established a TCP connection and the two peers have agreed to speak BGP with each other.
dropped	Number of times that a good connection has failed or been taken down.
Last reset	Elapsed time (in hours:minutes:seconds) since this peering session was last reset.
Connection state	State of the BGP Peer
unread input bytes	Number of bytes of packets still to be processed.
Local host, Local port	Peering address of the local router, plus the port.
Foreign host, Foreign port	Peering address of the neighbor.
Event Timers	Table that displays the number of starts and wakeups for each timer.
snduna	Last send sequence number for which the local host sent but has not received an acknowledgment.
sndnxt	Sequence number the local host will send next.
sndwnd	TCP window size of the remote host.

Field	Description
irs	Initial receive sequence number.
rcvnxt	Last receive sequence number the local host has acknowledged.
rcvwnd	TCP window size of the local host.
delrecvwnd	Delayed receive window--data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT	A calculated smoothed round-trip timeout (in milliseconds).
RTTO	Round-trip timeout (in milliseconds).
RTV	Variance of the round-trip time (in milliseconds).
KRTT	New round-trip timeout (in milliseconds) using the Karn algorithm. This field separately tracks the round-trip time of packets that have been re-sent.
minRTT	Smallest recorded round-trip timeout (in milliseconds) with hard wire value used for calculation.
maxRTT	Largest recorded round-trip timeout (in milliseconds).
ACK hold	Time (in milliseconds) the local host will delay an acknowledgment in order to "piggyback" data on it.
Flags	IP precedence of the BGP packets.
Datagrams: Rcvd	Number of update packets received from neighbor.
with data	Number of update packets received with data.
total data bytes	Total number of bytes of data.
Sent	Number of update packets sent.
with data	Number of update packets with data sent.
total data bytes	Total number of data bytes.

The following is sample output from the **show bgp ipv6 neighbors** command with the **advertised-routes** keyword:

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 advertised-routes
BGP table version is 21880, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*> 2001:208::/35    3FFE:C00:E:B::2                        0 237 7610 i
*> 2001:218::/35    3FFE:C00:E:C::2                        0 3748 4697 i
```

b

The following is sample output from the **show bgp ipv6 neighbors** command with the **routes** keyword:

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 routes
BGP table version is 21885, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 2001:200::/35    3FFE:700:20:1::11                      0 293 3425 2500 i
*  2001:208::/35    3FFE:700:20:1::11                      0 293 7610 i
*  2001:218::/35    3FFE:700:20:1::11                      0 293 3425 4697 i
*  2001:230::/35    3FFE:700:20:1::11                      0 293 1275 3748 i
Table below describes the significant fields shown in the display.
```

Table 21: show bgp ipv6 neighbors advertised-routes and routes fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.

Field	Description
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

The following is sample output from the **show bgp ipv6 neighbors** command with the **paths** keyword:

```
ciscoasa# show bgp ipv6 unicast neighbors 3FFE:700:20:1::11 paths ^293
Address    Refcount Metric Path
0x6131D7DC        2      0 293 3425 2500 i
0x6132861C        2      0 293 7610 i
0x6131AD18        2      0 293 3425 4697 i
0x61324084        2      0 293 1275 3748 i
0x61320E0C        1      0 293 3425 2500 2497 i
0x61326928        1      0 293 3425 2513 i
0x61327BC0        2      0 293 i
0x61321758        1      0 293 145 i
0x61320BEC        1      0 293 3425 6509 i
0x6131AAF8        2      0 293 1849 2914 ?
0x61320FE8        1      0 293 1849 1273 209 i
0x613260A8        2      0 293 1849 i
0x6132586C        1      0 293 1849 5539 i
0x6131BBF8        2      0 293 1849 1103 i
0x6132344C        1      0 293 4554 1103 1849 1752 i
0x61324150        2      0 293 1275 559 i
0x6131E5AC        2      0 293 1849 786 i
0x613235E4        1      0 293 1849 1273 i
0x6131D028        1      0 293 4554 5539 8627 i
0x613279E4        1      0 293 1275 3748 4697 3257 i
0x61320328        1      0 293 1849 1273 790 i
0x6131EC0C        2      0 293 1275 5409 i
The table below describes the significant fields shown in the display.
```

show bgp ipv6 neighbors paths fields

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

The following sample output from the **show bgp ipv6 neighbors** command shows the received routes for IPv6 address 2000:0:0:4::2:

```
ciscoasa# show bgp ipv6 unicast neighbors 2000:0:0:4::2 received-routes
BGP table version is 2443, local router ID is 192.168.0.2
Status codes:s suppressed, h history, * valid, > best, i - internal
Origin codes:i - IGP, e - EGP, ? - incomplete
Network                Next Hop           Metric LocPrf Weight Path
*> 2000:0:0:1::/64      2000:0:0:4::2                       0 2 1 i
*> 2000:0:0:2::/64      2000:0:0:4::2                       0 2 i
*> 2000:0:0:2:1::/80    2000:0:0:4::2                       0 2 ?
*> 2000:0:0:3::/64      2000:0:0:4::2                       0 2 ?
*  2000:0:0:4::1/64     2000:0:0:4::2                       0 2 ?
```

show bgp ipv6 paths

To display all the IPv6 Border Gateway Protocol (BGP) paths in the database, use the **show bgp ipv6 paths** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast paths *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
regular-expression	Regular expression that is used to match the received paths in the database.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The **show bgp ipv6 unicast paths** command provide output similar to the **show ip bgp paths** command, except they are IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6 paths** command:

```
ciscoasa# show bgp ipv6 unicast paths
Address    Hash Refcount Metric Path
0x61322A78    0        2      0 i
0x6131C214    3        2      0 6346 8664 786 i
0x6131D600   13        1      0 3748 1275 8319 1273 209 i
0x613229F0   17        1      0 3748 1275 8319 12853 i
0x61324AE0   18        1      1 4554 3748 4697 5408 i
0x61326818   32        1      1 4554 5609 i
0x61324728   34        1      0 6346 8664 9009 ?
0x61323804   35        1      0 3748 1275 8319 i
0x61327918   35        1      0 237 2839 8664 ?
0x61320504   38        2      0 3748 4697 1752 i
0x61320988   41        2      0 1849 786 i
0x6132245C   46        1      0 6346 8664 4927 i
Table below describes the significant fields shown in the display.
```

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)
Path	The autonomous system path for that route, followed by the origin code for that route.

show bgp ipv6 prefix-list

To display routes that match a prefix list, use the **show bgp ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast prefix-list *name*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
name	The specified prefix-list

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The specified prefix list must be an IPv6 prefix list, which is similar in format to an IPv4 prefix list.

Example

```
The following is sample output from the show bgp ipv6 prefix-list
command:
Router# show bgp ipv6 unicast prefix-list pin
ipv6 prefix-list pin:
   count:4, range entries:3, sequences:5 - 20, refcount:2
   seq 5 permit 747::/16 (hit count:1, refcount:2)
   seq 10 permit 747:1::/32 ge 64 le 64 (hit count:2, refcount:2)
   seq 15 permit 747::/32 ge 33 (hit count:1, refcount:1)
   seq 20 permit 777::/16 le 124 (hit count:2, refcount:1)
The ipv6 prefix-list match the following prefixes:
   seq 5: matches the exact match 747::/16
   seq 10:first 32 bits in prefix must match with a prefixlen of /64
   seq 15:first 32 bits in prefix must match with any prefixlen up to /128
   seq 20:first 16 bits in prefix must match with any prefixlen up to /124
Table below describes the significant fields shown in the display.
```

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 quote-regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression as a quoted string of characters, use the **show bgp ipv6 quote-regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast quote-regexp *regular expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
regular expression	Regular expression that is used to match the BGP autonomous system paths

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The **show bgp ipv6 unicast quote-regexp** command provide output similar to the **show ip bgp quote-regexp** command, except they are IPv6-specific.

Example

The following is sample output from the **show bgp ipv6 quote-regexp** command that shows paths beginning with 33 or containing 293:

```
Router# show bgp ipv6 unicast quote-regexp ^33|293
BGP table version is 69964, local router ID is 192.31.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
* 3FFE:C00:E:F::2                        0 6389 1849 293 1275
Table below describes the significant fields shown in the display.
```

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 regexp

To display IPv6 Border Gateway Protocol (BGP) routes matching the autonomous system path regular expression, use the **show bgp ipv6 regexp** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast regexp *regular-expression*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
regular-expression	Regular expression that is used to match the BGP autonomous system paths

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The **show bgp ipv6 unicast regexp** command provide output similar to the **show ip bgp regexp** command, except they are IPv6-specific.

Example

The following is sample output from the **show bgp ipv6 regexp** command that shows paths beginning with 33 or containing 293:

```
Router# show bgp ipv6 unicast regexp ^33|293
BGP table version is 69964, local router ID is 192.168.7.225
Status codes: s suppressed, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*  2001:200::/35    3FFE:C00:E:4::2          1             0 4554 293 3425 2500 i
*                   2001:0DB8:0:F004::1
                                                           0 3320 293 3425 2500 i
*  2001:208::/35    3FFE:C00:E:4::2          1             0 4554 293 7610 i
*  2001:228::/35    3FFE:C00:E:F::2                        0 6389 1849 293 2713 i
*  3FFE::/24        3FFE:C00:E:5::2                        0 33 1849 4554 i
*  3FFE:100::/24    3FFE:C00:E:5::2                        0 33 1849 3263 i
*  3FFE:300::/24    3FFE:C00:E:5::2                        0 33 293 1275 1717 i
*                   3FFE:C00:E:F::2                        0 6389 1849 293 1275
Table below describes the significant fields shown in the display.
```

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 route-map

To display IPv6 Border Gateway Protocol (BGP) routes that failed to install in the routing table, use the **show bgp ipv6 route-map** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast route-map *name*

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.
name	A specified route map to match.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The following is sample output from the **show bgp ipv6 route-map** command for a route map named rmap:

```
Router# show bgp ipv6 unicast route-map rmap
BGP table version is 16, local router ID is 172.30.242.1
Status codes:s suppressed, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes:i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i12:12::/64       2001:0DB8:101::1            0    100     50 ?
*>i12:13::/64       2001:0DB8:101::1            0    100     50 ?
*>i12:14::/64       2001:0DB8:101::1            0    100     50 ?
*>i543::/64         2001:0DB8:101::1            0    100     50 ?
```

The table below describes the significant fields shown in the display:

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	A 32-bit number written as 4 octets separated by periods (dotted-decimal format).

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. h—The table entry is history. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP.

show bgp ipv6 summary

To display the status of all IPv6 Border Gateway Protocol (BGP) connections, use the **show bgp ipv6 summary** command in user EXEC or privileged EXEC mode.

show bgp ipv6 unicast summary

Syntax Description

unicast	Specifies IPv6 unicast address prefixes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.3(2)	This command was added

Examples

The **show bgp ipv6 unicast summary** command provides output similar to the **show ip bgp summary** command, except they are IPv6-specific.

Examples

The following is sample output from the **show bgp ipv6 summary** command:

```
ciscoasa# show bgp ipv6 unicast summary
BGP device identifier 172.30.4.4, local AS number 200
BGP table version is 1, main routing table version 1
Neighbor          V    AS  MsgRcvd  MsgSent   TblVer  InQ  OutQ  Up/Down   State/PfxRcd
2001:0DB8:101::2  4    200    6869     6882        0    0     0  06:25:24  Active
```

The table below describes the significant fields shown in the display.

Field	Description
BGP device identifier	IP address of the networking device.
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
main routing table version	Last version of BGP database that was injected into the main routing table.

Field	Description
Neighbor	IPv6 address of a neighbor.
V	BGP version number spoken to that neighbor.
AS	Autonomous System
MsgRcvd	BGP messages received from that neighbor.
MsgSent	BGP messages sent to that neighbor
TblVer	Last version of the BGP database that was sent to that neighbor.
InQ	Number of messages from that neighbor waiting to be processed.
OutQ	Number of messages waiting to be sent to that neighbor.
Up/Down	The length of time that the BGP session has been in state Established, or the current state if it is not Established.
State/PfxRcd	Current state of the BGP session/the number of prefixes the device has received from a neighbor. When the maximum number (as set by the **neighbor maximum-prefix** command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the **neighbor shutdown** command.

show bgp neighbors

To display information about Border Gateway Protocol (BGP) and TCP connections to neighbors, use the show bgp neighbors command in user or privileged EXEC mode.

show bgp neighbors [**slow** | *ip-address* [**advertised-routes | | paths** [*reg-exp* **| policy** [**detail**] **|** **received prefix-filter | received-routes | routes**]]

Syntax Description

slow	(Optional) Displays information about dynamically configured slow peers
ip-address	(Optional) Displays information about the IPv4 neighbor. If this argument is omitted, information about all neighbors is displayed.
advertised-routes	(Optional) Displays all routes that have been advertised to neighbors.
paths reg-exp	(Optional) Displays autonomous system paths learned from the specified neighbor. An optional regular expression can be used to filter the output.
policy	(Optional) Displays the policies applied to this neighbor per address family.
detail	(Optional) Displays detailed policy information such as route maps, prefix lists, community lists, access control lists (ACLs), and autonomous system path filter lists.
received prefix-filter	(Optional) Displays the prefix-list (outbound route filter [ORF]) sent from the specified neighbor.
received-routes	(Optional) Displays all received routes (both accepted and rejected) from the specified neighbor.
routes	(Optional) Displays all routes that are received and accepted. The output displayed when this keyword is entered is a subset of the output displayed by the received-routes keyword.

Command Default

The output of this command displays information for all neighbors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

Use the show bgp neighbors command to display BGP and TCP connection information for neighbor sessions. For BGP, this includes detailed neighbor attribute, capability, path, and prefix information. For TCP, this includes statistics related to BGP neighbor session establishment and maintenance.

Prefix activity is displayed based on the number of prefixes that are advertised and withdrawn. Policy denials display the number of routes that were advertised but then ignored based on the function or attribute that is displayed in the output.

Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command followed by the clear bgp * command to perform a hard reset of all current BGP sessions.

Examples

Example output is different for the various keywords available for the show bgp neighbors command. Examples using the various keywords appear in the following sections:

show bgp neighbors: Example

The following example shows output for the BGP neighbor at 10.108.50.2. This neighbor is an internal BGP (iBGP) peer. This neighbor supports the route refresh and graceful restart capabilities.

```
ciscoasa# show bgp neighbors 10.108.50.2
BGP neighbor is 10.108.50.2,  remote AS 1, internal link
  BGP version 4, remote router ID 192.168.252.252
  BGP state = Established, up for 00:24:25
  Last read 00:00:24, last write 00:00:24, hold time is 180, keepalive interval is
   60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(old & new)
    MPLS Label capability: advertised and received
    Graceful Restart Capability: advertised
    Address family IPv4 Unicast: advertised and received
  Message statistics:
    InQ depth is 0
    OutQ depth is 0
                         Sent       Rcvd
    Opens:                  3          3
    Notifications:          0          0
    Updates:                0          0
    Keepalives:           113        112
    Route Refresh:          0          0
    Total:                116        115
  Default minimum time between advertisement runs is 5 seconds
 For address family: IPv4 Unicast
  BGP additional-paths computation is enabled
  BGP advertise-best-external is enabled
  BGP table version 1, neighbor version 1/0
 Output queue size : 0
  Index 1, Offset 0, Mask 0x2
  1 update-group member
                                 Sent       Rcvd
  Prefix activity:               ----       ----
    Prefixes Current:               0          0
    Prefixes Total:                 0          0
    Implicit Withdraw:              0          0
    Explicit Withdraw:              0          0
    Used as bestpath:             n/a          0
    Used as multipath:            n/a          0
```

```
                                   Outbound    Inbound
  Local Policy Denied Prefixes:    --------    -------
    Total:                                0          0
  Number of NLRIs in the update sent: max 0, min 0
  Connections established 3; dropped 2
  Last reset 00:24:26, due to Peer closed the session
External BGP neighbor may be up to 2 hops away.
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
Connection is ECN Disabled
Local host: 10.108.50.1, Local port: 179
Foreign host: 10.108.50.2, Foreign port: 42698
Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)
Event Timers (current time is 0x68B944):
Timer          Starts    Wakeups            Next
Retrans            27          0             0x0
TimeWait            0          0             0x0
AckHold            27         18             0x0
SendWnd             0          0             0x0
KeepAlive           0          0             0x0
GiveUp              0          0             0x0
PmtuAger            0          0             0x0
DeadWait            0          0             0x0
iss: 3915509457  snduna: 3915510016  sndnxt: 3915510016     sndwnd:  15826
irs:  233567076  rcvnxt:  233567616  rcvwnd:      15845  delrcvwnd:    539
SRTT: 292 ms, RTTO: 359 ms, RTV: 67 ms, KRTT: 0 ms
minRTT: 12 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs
IP Precedence value : 6
Datagrams (max data segment is 1460 bytes):
Rcvd: 38 (out of order: 0), with data: 27, total data bytes: 539
Sent: 45 (retransmit: 0, fastretransmit: 0, partialack: 0, Second Congestion: 08
```

Below table describes the significant fields shown in the display. Fields that are preceded by the asterisk character (*) are displayed only when the counter has a nonzero value.

Table 14: show bgp ipv4 Fields shows each field description.

Table 22: show bgp ipv4 Fields

Field	**Description**
BGP neighbor	IP address of the BGP neighbor and its autonomous system number.
remote AS	Autonomous system number of the neighbor.
local AS 300 no-prepend (not shown in display)	Verifies that the local autonomous system number is not prepended to received external routes. This output supports the hiding of the local autonomous systems when migrating autonomous systems.
internal link	"internal link" is displayed for iBGP neighbors. "external link" is displayed for external BGP (eBGP) neighbors.
BGP version	BGP version being used to communicate with the remote router.
remote router ID	IP address of the neighbor.
BGP state	Finite state machine (FSM) stage of session negotiation.

Field	Description
up for	Time, in hhmmss, that the underlying TCP connection has been in existence.
Last read	Time, in hhmmss, since BGP last received a message from this neighbor.
last write	Time, in hhmmss, since BGP last sent a message to this neighbor.
hold time	Time, in seconds, that BGP will maintain the session with this neighbor without receiving a messages.
keepalive interval	Time interval, in seconds, at which keepalive messages are transmitted to this neighbor.
Neighbor capabilities	BGP capabilities advertised and received from this neighbor. “advertised and received” is displayed when a capability is successfully exchanged between two routers
Route Refresh	Status of the route refresh capability.
Graceful Restart Capability	Status of the graceful restart capability.
Address family IPv4 Unicast	IP Version 4 unicast-specific properties of this neighbor.
Message statistics	Statistics organized by message type.
InQ depth is	Number of messages in the input queue.
OutQ depth is	Number of messages in the output queue.
Sent	Total number of transmitted messages.
Received	Total number of received messages.
Opens	Number of open messages sent and received.
notifications	Number of notification (error) messages sent and received.
Updates	Number of update messages sent and received.
Keepalives	Number of keepalive messages sent and received.
Route Refresh	Number of route refresh request messages sent and received.
Total	Total number of messages sent and received.
Default minimum time between...	Time, in seconds, between advertisement transmissions.
For address family:	Address family to which the following fields refer.
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.

Field	Description
neighbor version	Number used by the software to track prefixes that have been sent and those that need to be sent.
update-group	Number of update-group member for this address family
Prefix activity	Prefix statistics for this address family.
Prefixes current	Number of prefixes accepted for this address family.
Prefixes total	Total number of received prefixes.
Implicit Withdraw	Number of times that a prefix has been withdrawn and readvertised.
Explicit Withdraw	Number of times that prefix has been withdrawn because it is no longer feasible.
Used as bestpath	Number of received prefixes installed as bestpaths.
Used as multipath	Number of received prefixes installed as multipaths.
* Saved (soft-reconfig)	Number of soft resets performed with a neighbor that supports soft reconfiguration. This field is displayed only if the counter has a nonzero value.
* History paths	This field is displayed only if the counter has a nonzero value.
* Invalid paths	Number of invalid paths. This field is displayed only if the counter has a nonzero value.
Local Policy Denied Prefixes	Prefixes denied due to local policy configuration. Counters are updated for inbound and outbound policy denials. The fields under this heading are displayed only if the counter has a nonzero value.
* route-map	Displays inbound and outbound route-map policy denials.
* filter-list	Displays inbound and outbound filter-list policy denials.
* prefix-list	Displays inbound and outbound prefix-list policy denials.
* AS_PATH too long	Displays outbound AS-path length policy denials.
* AS_PATH loop	Displays outbound AS-path loop policy denials.
* AS_PATH confed info	Displays outbound confederation policy denials.
* AS_PATH contains AS 0	Displays outbound denials of autonomous system (AS) 0.
* NEXT_HOP Martian	Displays outbound martian denials.
* NEXT_HOP non-local	Displays outbound non-local next-hop denials.
* NEXT_HOP is us	Displays outbound next-hop-self denials.
* CLUSTER_LIST loop	Displays outbound cluster-list loop denials.

Field	Description
* ORIGINATOR loop	Displays outbound denials of local originated routes.
* unsuppress-map	Displays inbound denials due to an unsuppress-map.
* advertise-map	Displays inbound denials due to an advertise-map.
* Well-known Community	Displays inbound denials of well-known communities.
* SOO loop	Displays inbound denials due to site-of-origin.
* Bestpath from this peer	Displays inbound denials because the bestpath came from the local router.
* Suppressed due to dampening	Displays inbound denials because the neighbor or link is in a dampening state.
* Bestpath from iBGP peer	Deploys inbound denials because the bestpath came from an iBGP neighbor.
* Incorrect RIB for CE	Deploys inbound denials due to RIB errors for a CE router.
* BGP distribute-list	Displays inbound denials due to a distribute list.
Number of NLRIs...	Number of network layer reachability attributes in updates.
Connections established	Number of times a TCP and BGP connection has been successfully established.
dropped	Number of times that a valid session has failed or been taken down.
Last reset	Time since this peering session was last reset. The reason for the reset is displayed on this line.
External BGP neighbor may be... (not shown in the display)	Indicates that the BGP TTL security check is enabled. The maximum number of hops that can separate the local and remote peer is displayed on this line.
Connection state	Connection status of the BGP peer.
Connection is ECN Disabled	Explicit congestion notification status (enabled or disabled).
Local host: 10.108.50.1, Local port: 179	IP address of the local BGP speaker. BGP port number 179.
Foreign host: 10.108.50.2, Foreign port: 42698	Neighbor address and BGP destination port number.
Enqueued packets for retransmit:	Packets queued for retransmission by TCP.
Event Timers	TCP event timers. Counters are provided for starts and wakeups (expired timers).
Retrans	Number of times a packet has been retransmitted.

Field	Description
TimeWait	Time waiting for the retransmission timers to expire.
AckHold	Acknowledgment hold timer.
SendWnd	Transmission (send) window.
KeepAlive	Number of keepalive packets.
GiveUp	Number times a packet is dropped due to no acknowledgment.
PmtuAger	Path MTU discovery timer
DeadWait	Expiration timer for dead segments.
iss:	Initial packet transmission sequence number.
snduna	Last transmission sequence number that has not been acknowledged.
sndnxt:	Next packet sequence number to be transmitted.
sndwnd:	TCP window size of the remote neighbor.
irs:	Initial packet receive sequence number.
rcvnxt:	Last receive sequence number that has been locally acknowledged.
rcvwnd:	TCP window size of the local host.
delrcvwnd:	Delayed receive window—data the local host has read from the connection, but has not yet subtracted from the receive window the host has advertised to the remote host. The value in this field gradually increases until it is larger than a full-sized packet, at which point it is applied to the rcvwnd field.
SRTT:	A calculated smoothed round-trip timeout.
RTTO:	Round-trip timeout.
RTV:	Variance of the round-trip time.
KRTT:	New round-trip timeout (using the Karn algorithm). This field separately tracks the round-trip time of packets that have been re-sent.
minRTT:	Smallest recorded round-trip timeout (hard-wire value used for calculation).
maxRTT:	Largest recorded round-trip timeout.
ACK hold:	Length of time the local host will delay an acknowledgment to carry (piggyback) additional data.
IP Precedence value:	IP precedence of the BGP packets.
Datagrams	Number of update packets received from a neighbor.

Field	Description
Rcvd:	Number of received packets.
with data	Number of update packets sent with data.
total data bytes	Total amount of data received, in bytes.
Sent	Number of update packets sent.
Second Congestion	Number of second retransmissions sent due to congestion.
Datagrams: Rcvd	Number of update packets received from a neighbor.
out of order:	Number of packets received out of sequence.
with data	Number of update packets received with data.
Last reset	Elapsed time since this peering session was last reset.
unread input bytes	Number of bytes of packets still to be processed.
retransmit	Number of packets retransmitted.
fastretransmit	Number of duplicate acknowledgments retransmitted for an out of order segment before the retransmission timer expires.
partialack	Number of retransmissions for partial acknowledgments (transmissions before or without subsequent acknowledgments).

show bgp neighbors advertised-routes: Example

The following example displays routes advertised for only the 172.16.232.178 neighbor:

```
ciscoasa# show bgp neighbors 172.16.232.178 advertised-routes
BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Network          Next Hop          Metric LocPrf Weight Path
*>i10.0.0.0      172.16.232.179         0    100      0 ?
*> 10.20.2.0     10.0.0.0               0         32768 i
```

Table 23: show bgp neighbors advertised routes Fields shows each field description.

Table 23: show bgp neighbors advertised routes Fields

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: s—The table entry is suppressed. *—The table entry is valid. >—The table entry is the best entry to use for that network. i—The table entry was learned via an internal BGP (iBGP) session.
Origin codes	Origin of the entry. The origin code is placed at the end of each line in the table. It can be one of the following values: i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. e—Entry originated from an Exterior Gateway Protocol (EGP). ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	Internet address of the network the entry describes.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the access server has some non-BGP route to this network.
Metric	If shown, the value of the inter autonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path. At the end of the path is the origin code for the path: i—The entry was originated with the IGP and advertised with a network router configuration command. e—The route originated with EGP. ?—The origin of the path is not clear. Usually this is a path that is redistributed into BGP from an IGP..

Examples

show bgp neighbors paths: Example

The following is example output from the show bgp neighbors command entered with the paths keyword:

```
ciscoasa# show bgp neighbors 172.29.232.178 paths ^10
Address    Refcount Metric Path
0x60E577B0        2     40 10 ?
```

Table 24: show bgp neighbors paths Fields shows each field description.

Table 24: show bgp neighbors paths Fields

Field	Description
Address	Internal address where the path is stored.
Refcount	Number of routes using that path..
Metric	Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.).
Path	Autonomous system path for that route, followed by the origin code for that route..

Examples

show bgp neighbors received prefix-filter: Example

The following example shows that a prefix-list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor:

```
ciscoasa# show bgp neighbors 192.168.20.72 received prefix-filter
Address family:IPv4 Unicast
ip prefix-list 192.168.20.72:1 entries
   seq 5 deny 10.0.0.0/8 le 32
```

Table 25: show bgp neighbors received prefix filter Fields shows each field description.

Table 25: show bgp neighbors received prefix filter Fields

Field	Description
Address family	Address family mode in which the prefix filter is received.
ip prefix-list	Prefix list sent from the specified neighbor.

Examples

show bgp neighbors policy: Example

The following sample output shows the policies applied to the neighbor at 192.168.1.2. The output displays policies configured on the neighbor device.

```
ciscoasa# show bgp neighbors 192.168.1.2 policy
Neighbor: 192.168.1.2, Address-Family: IPv4 Unicast
Locally configured policies:
 route-map ROUTE in
Inherited polices:
 prefix-list NO-MARKETING in
 route-map ROUTE in
 weight 300
 maximum-prefix 10000
```

show bgp neighbors: Example

The following is sample output from the show bgp neighbors command that verifies that BGP TCP path maximum transmission unit (MTU) discovery is enabled for the BGP neighbor at 172.16.1.2:

```
ciscoasa# show bgp neighbors 172.16.1.2
BGP neighbor is 172.16.1.2,  remote AS 45000, internal link
  BGP version 4, remote router ID 172.16.1.99
.
.
.
 For address family: IPv4 Unicast
  BGP table version 5, neighbor version 5/0
.
.
.
  Address tracking is enabled, the RIB does have a route to 172.16.1.2
  Address tracking requires at least a /24 route to the peer
  Connections established 3; dropped 2
  Last reset 00:00:35, due to Router ID changed
  Transport(tcp) path-mtu-discovery is enabled
.
.
.
SRTT: 146 ms, RTTO: 1283 ms, RTV: 1137 ms, KRTT: 0 ms
minRTT: 8 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: higher precedence, retransmission timeout, nagle, path mtu capable
```

The following is partial output from the show bgp neighbors command that verifies the status of the BGP graceful restart capability for the external BGP peer at 192.168.3.2. Graceful restart is shown as disabled for this BGP peer.

```
ciscoasa# show bgp neighbors 192.168.3.2
BGP neighbor is 192.168.3.2,  remote AS 50000, external link
 Inherits from template S2 for session parameters
  BGP version 4, remote router ID 192.168.3.2
  BGP state = Established, up for 00:01:41
  Last read 00:00:45, last write 00:00:45, hold time is 180, keepalive intervals
  Neighbor sessions:
    1 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
.
.
.
Address tracking is enabled, the RIB does have a route to 192.168.3.2
  Connections established 1; dropped 0
  Last reset never
  Transport(tcp) path-mtu-discovery is enabled
  Graceful-Restart is disabled
Connection state is ESTAB, I/O status: 1, unread input bytes: 0
```

show bgp paths

To display all the BGP paths in the database, use the show bgp paths command in EXEC mode.

show bgp paths
Cisco 10000 Series Router
show bgp paths *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the show bgp paths command in privileged EXEC mode:

```
ciscoasa# show bgp paths
Address    Hash Refcount Metric Path
0x60E5742C    0        1      0 i
0x60E3D7AC    2        1      0 ?
0x60E5C6C0   11        3      0 10 ?
0x60E577B0   35        2     40 10 ?
```

Table 26: show bgp paths Fields shows each field description.

Table 26: show bgp paths Fields

Field	Description
Address	Internal address where the path is stored.
Hash	Hash bucket where path is stored.
Refcount	Number of routes using that path.
Metric	The Multi Exit Discriminator (MED) metric for the path. (The name of this metric for BGP versions 2 and 3 is INTER_AS.)

Field	Description
Path	The autonomous system path for that route, followed by the origin code for that route.

show bgp policy-list

To display information about a configured policy list and policy list entries, use the show bgp policy-list command in user EXEC mode.

show bgp policy-list [*policy-list-name*]

Syntax Description

policy-list-name	(Optional) Displays information about the specified policy list with this argument.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is sample output from the show bgp policy-list command. The output of this command will display the policy-list name and configured match clauses. The following sample output is similar to the output that will be displayed:

```
ciscoasa# show bgp policy-list
policy-list POLICY-LIST-NAME-1 permit
  Match clauses:
    metric 20
policy-list POLICY-LIST-NAME-2 permit
  Match clauses:
    as-path (as-path filter): 1
```

show bgp prefix-list

To display information about a prefix list or prefix list entries, use the show bgp prefix-list command in user or privileged EXEC mode

show bgp prefix-list [**detail | summary**] [*prefix-list-name* [**seq** *sequence-number* | *network/length* [**longer|first-match**]]]

Syntax Description

detail | summary	(Optional) Displays detailed or summarized information about all prefix lists.
first-match	(Optional) Displays the first entry of the specified prefix list that matches the given network/length.
longer	(Optional) Displays all entries of the specified prefix list that match or are more specific than the given network/length.
network/length	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits).
prefix-list-name	(Optional) Displays the entries in a specific prefix list.
seq sequence-number	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix-list.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following example shows the output of the show bgp prefix-list command with details about the prefix list named test:

```
ciscoasa# show bgp prefix-list detail test
ip prefix-list test:
Description: test-list
 count: 1, range entries: 0, sequences: 10 - 10, refcount: 3
 seq 10 permit 10.0.0.0/8 (hit count: 0, refcount: 1)
```

show bgp regexp

To display routes matching the autonomous system path regular expression, use the show bgp regexp command in EXEC mode.

show bgp regexp *regexp*

Syntax Description

regexp	Regular expression to match the BGP autonomous system paths. For more details about autonomous system number formats, see the router bgp command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command followed by the clear bgp * command to perform a hard reset of all current BGP sessions.

To ensure a smooth transition we recommend that all BGP speakers within an autonomous system that is identified using a 4-byte autonomous system number, are upgraded to support 4-byte autonomous system numbers.

Examples

The following is sample output from the show bgp regexp command in privileged EXEC mode:

```
Router# show bgp regexp 108$
BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop          Metric LocPrf Weight Path
*  172.16.0.0       172.16.72.30                         0 109 108 ?
*  172.16.1.0       172.16.72.30                         0 109 108 ?
*  172.16.11.0      172.16.72.30                         0 109 108 ?
*  172.16.14.0      172.16.72.30                         0 109 108 ?
*  172.16.15.0      172.16.72.30                         0 109 108 ?
*  172.16.16.0      172.16.72.30                            0 109 108 ?
*  172.16.17.0      172.16.72.30                            0 109 108 ?
*  172.16.18.0      172.16.72.30                            0 109 108 ?
*  172.16.19.0      172.16.72.30                            0 109 108 ?
*  172.16.24.0      172.16.72.30                            0 109 108 ?
*  172.16.29.0      172.16.72.30                            0 109 108 ?
*  172.16.30.0      172.16.72.30                            0 109 108 ?
*  172.16.33.0      172.16.72.30                            0 109 108 ?
*  172.16.35.0      172.16.72.30                            0 109 108 ?
*  172.16.36.0      172.16.72.30                            0 109 108 ?
*  172.16.37.0      172.16.72.30                            0 109 108 ?
*  172.16.38.0      172.16.72.30                            0 109 108 ?
*  172.16.39.0      172.16.72.30                            0 109 108 ?
```

After the bgp asnotation dot command is configured, the regular expression match format for 4-byte autonomous system paths is changed to asdot notation format. Although a 4-byte autonomous system number can be configured in a regular expression using either asplain or asdot format, only 4-byte autonomous system numbers configured using the current default format are matched. In the first example, the show bgp regexp command is configured with a 4-byte autonomous system number in asplain format. The match fails because the default format is currently asdot format and there is no output. In the second example using asdot format, the match passes and the information about the 4-byte autonomous system path is shown using the asdot notation.

Note The asdot notation uses a period which is a special character in Cisco regular expressions. to remove the special meaning, use a backslash before the period.

```
Router# show bgp regexp ^65536$
Router# show bgp regexp ^1\.0$
BGP table version is 2, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.0 i
```

The following is sample output from the show bgp regexp command after the bgp asnotation dot command has been entered to display 4-byte autonomous system numbers

Note The asdot notation uses a period which is a special character in Cisco regular expressions. to remove the special meaning, use a backslash before the period.

```
Router# show bgp regexp ^1\.14$
BGP table version is 4, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.1.1.0/24      192.168.1.2              0             0 1.14   i
```

show bgp replication

To display update replication statistics for Border Gateway Protocol (BGP) update groups, use the show bgp replication command in EXEC mode.

show bgp replication [*index-group* | *ip-address*]

Syntax Description

index-group	(Optional) Displays update replication statistics for the update group with the corresponding index number. The range of update-group index numbers is from 1 to 4294967295.
ip-address	(Optional) Displays update replication statistics for this neighbor.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

The output of this command displays BGP update-group replication statistics.

When a change to outbound policy occurs, the router automatically recalculates update-group memberships and applies the changes by triggering an outbound soft reset after a 3-minute timer expires. This behavior is designed to provide the network operator with time to change the configuration if a mistake is made. You can manually enable an outbound soft reset before the timer expires by entering the clearbgp ip-address soft out command.

Examples

The following sample output from the show bgp replication command shows update-group replication information for all neighbors:

```
ciscoasa# show bgp replication
BGP Total Messages Formatted/Enqueued : 0/0
     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         1 internal        1       10.4.9.21        0        0      0      0
         2 internal        2        10.4.9.5        0        0      0      0
The following sample output from the show bgp replication command shows update-group
statistics for the 10.4.9.5 neighbor:
Router# show bgp replication 10.4.9.5
     Index     Type  Members          Leader   MsgFmt  MsgRepl  Csize  Qsize
         2 internal        2        10.4.9.5        0        0      0      0
```

Table 27: show bgp replication Fields shows each field description.

Table 27: show bgp replication Fields

Field	Description
Index	Index number of the update group.
Type	Type of peer (internal or external).
Members	Number of members in the dynamic update peer group.
Leader	First member of the dynamic update peer group.

show bgp rib-failure

To display Border Gateway Protocol (BGP) routes that failed to install in the Routing Information Base (RIB) table, use the show bgp rib-failure command in privileged EXEC mode.

show bgp rib-failure

Syntax Description

This command has no keywords or arguments.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Examples

The following is a sample output from the show bgp rib-failure command:

```
ciscoasa# show bgp rib-failure
Network            Next Hop                      RIB-failure   RIB-NH Matches
10.1.15.0/24       10.1.35.5         Higher admin distance              n/a
10.1.16.0/24       10.1.15.1         Higher admin distance              n/a
```

Table 28: show bgp rib-failure Fields shows each field description.

Table 28: show bgp rib-failure Fields

Field	Description
Network	IP address of a network entity
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of RIB failure. Higher admin distance means that a route with a better (lower) administrative distance such as a static route already exists in the IP routing table.

Field	Description
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and bgp suppress-inactive is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or next hop recurses down to the same adjacency as the BGP nexthop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that bgp suppress-inactive is not configured for the address family being used.

show bgp summary

To display the status of all Border Gateway Protocol (BGP) connections, use the show bgp summary command in user EXEC or privileged EXEC mode.

show bgp summary

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

The show bgp summary command is used to display BGP path, prefix, and attribute information for all connections to BGP neighbors.

A prefix is an IP address and network mask. It can represent an entire network, a subset of a network, or a single host route. A path is a route to a given destination. By default, BGP will install only a single path for each destination. If multipath routes are configured, BGP will install a path entry for each multipath route, and only one multipath route will be marked as the bestpath.

BGP attribute and cache entries are displayed individually and in combinations that affect the bestpath selection process. The fields for this output are displayed when the related BGP feature is configured or attribute is received. Memory usage is displayed in bytes.

The Cisco implementation of 4-byte autonomous system numbers uses asplain—65538 for example—as the default regular expression match and output display format for autonomous system numbers, but you can configure 4-byte autonomous system numbers in both the asplain format and the asdot format as described in RFC 5396. To change the default regular expression match and output display of 4-byte autonomous system numbers to asdot format, use the bgp asnotation dot command followed by the clear bgp * command to perform a hard reset of all current BGP sessions.

Examples

The following is sample output from the show bgp summary command in privileged EXEC mode:

```
Router# show bgp summary
BGP router identifier 172.16.1.1, local AS number 100
BGP table version is 199, main routing table version 199
37 network entries using 2850 bytes of memory
59 path entries using 5713 bytes of memory
18 BGP path attribute entries using 936 bytes of memory
```

```
2 multipath network entries and 4 multipath paths
10 BGP AS-PATH entries using 240 bytes of memory
7 BGP community entries using 168 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
90 BGP advertise-bit cache entries using 1784 bytes of memory
36 received paths for inbound soft reconfiguration
BGP using 34249 total bytes of memory
Dampening enabled. 4 history paths, 0 dampened paths
BGP activity 37/2849 prefixes, 60/1 paths, scan interval 15 secs
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down State/PfxRcd
10.100.1.1      4   200      26      22      199    0    0 00:14:23 23
10.200.1.1      4   300      21      51      199    0    0 00:13:40 0
```

Table 29: show bgp summary Fields shows each field description.

Table 29: show bgp summary Fields

Field	Description
BGP router identifier	In order of precedence and availability, the router identifier specified by the bgp router-id command, a loopback address, or the highest IP address.
BGP table version	Internal version number of BGP database.
main routing table version	Last version of BGP database that was injected into the main routing table.
...network entries	Number of unique prefix entries in the BGP database.
...using ... bytes of memory	Amount of memory, in bytes, that is consumed for the path, prefix, or attribute entry displayed on the same line.
...path entries using	Number of path entries in the BGP database. Only a single path entry will be installed for a given destination. If multipath routes are configured, a path entry will be installed for each multipath route.
...multipath network entries using	Number of multipath entries installed for a given destination.
* ...BGP path/bestpath attribute entries using	Number of unique BGP attribute combinations for which a path is selected as the bestpath.
* ...BGP rrinfo entries using	Number of unique ORIGINATOR and CLUSTER_LIST attribute combinations.
...BGP AS-PATH entries using	Number of unique AS_PATH entries.
...BGP community entries using	Number of unique BGP community attribute combinations.
*...BGP extended community entries using	Number of unique extended community attribute combinations.
BGP route-map cache entries using	Number of BGP route-map match and set clause combinations. A value of 0 indicates that the route cache is empty.
...BGP filter-list cache entries using	Number of filter-list entries that match an AS-path access list permit or deny statements. A value of 0 indicates that the filter-list cache is empty.

Field	Description
BGP advertise-bit cache entries using	(Cisco IOS Release 12.4(11)T and later releases only) Number of advertised bitfield entries and the associated memory usage. A bitfield entry represents a piece of information (one bit) that is generated when a prefix is advertised to a peer. The advertised bit cache is built dynamically when required
...received paths for inbound soft reconfiguration	Number paths received and stored for inbound soft reconfiguration.
BGP using...	Total amount of memory, in bytes, used by the BGP process.
Dampening enabled...	Indicates that BGP dampening is enabled. The number of paths that carry an accumulated penalty and the number of dampened paths are displayed on this line.
BGP activity...	Displays the number of times that memory has been allocated or released for a path or prefix.
Neighbor	IP address of the neighbor.
V	BGP version number spoken to the neighbor.
AS	Autonomous system number.
MsgRcvd	Number of messages received from the neighbor.
MsgSent	Number of messages sent to the neighbor.
TblVer	Last version of the BGP database that was sent to the neighbor.
InQ	Number of messages queued to be processed from the neighbor.
OutQ	Number of messages queued to be sent to the neighbor.
Up/Down	The length of time that the BGP session has been in the Established state, or the current status if not in the Established state.
State/PfxRcd	Current state of the BGP session, and the number of prefixes that have been received from a neighbor or peer group. When the maximum number (as set by the neighbor maximum-prefix command) is reached, the string "PfxRcd" appears in the entry, the neighbor is shut down, and the connection is set to Idle. An (Admin) entry with Idle status indicates that the connection has been shut down using the neighbor shutdown command.

Examples

The following output from the show bgp summary command shows that the BGP neighbor 192.168.3.2 was dynamically created and is a member of the listen range group, group192. The output also shows that the IP prefix range of 192.168.0.0/16 is defined for the listen range group named group192. In Cisco IOS Release 12.2(33)SXH and later releases, the BGP dynamic neighbor feature added the ability to support the dynamic creation of BGP neighbor peers using a subnet range associated with a peer group (listen range group).

```
ciscoasa# show bgp summary
BGP router identifier 192.168.3.1, local AS number 45000
BGP table version is 1, main routing table version 1
Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
*192.168.3.2    4 50000       2       2        0    0    0 00:00:37        0
* Dynamically created based on a listen range command
Dynamically created neighbors: 1/(200 max), Subnet ranges: 1
BGP peergroup group192 listen range group members:
  192.168.0.0/16
```

The following output from the show bgp summary command shows two BGP neighbors, 192.168.1.2 and 192.168.3.2, in different 4-byte autonomous system numbers, 65536 and 65550. The local autonomous system 65538 is also a 4-byte autonomous system number and the numbers are displayed in the default asplain format.

```
Router# show bgp summary
BGP router identifier 172.17.1.99, local AS number 65538
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4       65536       7       7        1    0    0 00:03:04      0
192.168.3.2     4       65550       4       4        1    0    0 00:00:15      0
```

The following output from the show bgp summary command shows the same two BGP neighbors, but the 4-byte autonomous system numbers are displayed in asdot notation format. To change the display format the bgp asnotation dot command must be configured in router configuration mode.

```
Router# show bgp summary
BGP router identifier 172.17.1.99, local AS number 1.2
BGP table version is 1, main routing table version 1
Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
192.168.1.2     4         1.0       9       9        1    0    0 00:04:13      0
192.168.3.2     4        1.14       6       6        1    0    0 00:01:24      0
```

The following example displays sample output of the show bgp summary slow command:

```
ciscoasa> show bgp summary slow
BGP router identifier 2.2.2.2, local AS number 100
BGP table version is 37, main routing table version 37
36 network entries using 4608 bytes of memory
36 path entries using 1872 bytes of memory
1/1 BGP path/bestpath attribute entries using 124 bytes of memory
1 BGP rrinfo entries using 24 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
1 BGP extended community entries using 24 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6700 total bytes of memory
BGP activity 46/0 prefixes, 48/0 paths, scan interval 60 secs

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd
6.6.6.6 4 100 11 10 1 0 0 00:44:20 0
```

show bgp system-config

To display running configuration for bgp of system context in user context, use the show bgp system-config command in user or privileged EXEC mode.

show bgp system-config

Syntax Description

This command has no arguments or keywords.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC, User EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.2(1)	This command was added

Usage Guidelines

This command can be used only in user context without any arguments or keywords. This command can be useful for checking the running configuration enforced on user context by system context.

Examples

The following sample output is similar to the output that will be displayed when the show bgp system-config command is entered in user EXEC mode:

```
ciscoasa/c1(config)# show bgp system-config
router bgp 1
 bgp log-neighbor-changes
 no bgp always-compare-med
 no bgp asnotation dot
 no bgp bestpath med
 no bgp bestpath compare-routerid
 bgp default local-preference 100
 no bgp deterministic-med
 bgp enforce-first-as
 bgp maxas-limit 0
 bgp transport path-mtu-discovery
 timers bgp 60 180 0
 address-family ipv4 unicast
  bgp scan-time 0
  bgp nexthop trigger enable
  bgp nexthop trigger delay 5
 exit-address-family
```

show blocks

To show the packet buffer utilization, use the **show blocks** command in privileged EXEC mode.

show blocks [**core | export-failed | interface**] [{ **address** *hex* **| all | assigned | free | old | pool** *size* [**summary**] } [**diagnostics | dump | header | packet] | queue history |** [**exhaustion snapshot | history** [**list**] [*1-MAX_NUM_SNAPSHOT* | *index*] [**detail**]] [**depleted** *size*]

Syntax Description

address *hex*	(Optional) Shows a block corresponding to this address, in hexadecimal.
all	(Optional) Shows all blocks.
assigned	(Optional) Shows blocks that are assigned and in use by an application.
core	(Optional) Shows core-specific buffers.
depleted	(Optional) Shows the depleted block details for the specified block size. Valid sizes are 0, 4, 80, 256, 1550, 2560, 2048, 4096, 8192, 9344, 16384 and 65536/65664.
detail	(Optional) Shows a portion (128 bytes) of the first block for each unique queue type.
dump *	(Optional) Shows the entire block contents, including the header and packet information. The difference between dump and packet is that dump includes additional information between the header and the packet.
diagnostics	(Optional) Shows block diagnostics.
exhaustion snapshot	(Optional) Prints the last x number (x is currently 10) of snapshots that were taken and the time stamp of the last snapshot). After a snapshot is taken, another snapshot is not taken if less than 5 minutes has passed.
export-failed	(Optional) Show system buffer export failure counters.
free	(Optional) Shows blocks that are available for use.
header	(Optional) Shows the header of the block.
history *1-MAX_NUM_SNAPSHOT* **history** *index* **history list**	The **history** option displays recent and all snapshots in the history. The **history list** option displays a summary of snapshots in the history. The **history** *index* option displays the index of snapshots in the history. The **history** *1-MAX_NUM_SNAPSHOT* option displays only one snapshot in the history.
interface	(Optional) Show buffers attached to interfaces.
old *	(Optional) Shows blocks that were assigned more than a minute ago.
packet	(Optional) Shows the header of the block as well as the packet contents.

pool *size* *	(Optional) Shows blocks of a specific size.
queue history	(Optional) Shows where blocks are assigned when the ASA runs out of blocks. Sometimes, a block is allocated from the pool but never assigned to a queue. In that case, the location is the code address that allocated the block.
summary	(Optional) Shows detailed information about block usage sorted by the program addresses of applications that allocated blocks in this class, program addresses of applications that released blocks in this class, and the queues to which valid blocks in this class belong.

*When these commands are integrated in scripts and run within aggresive intervals, it might overload the system. Therefore, use these commands after verifying the system capacity to withstand the load.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	The **pool summary** option was added.
8.0(2)	The dupb block uses 0 length blocks now instead of 4 byte blocks. An additional line was added for 0 byte blocks.
9.1(5)	The **exhaustion snapshot** , **history list** , **history** *index,* and **history** *1-MAX_NUM_SNAPSHOT* options were added.
9.14(1)	The **depleted** keyword was added to the command to display the depleted block details.
9.16(2)	The output of this command was enhanced to include the failed count.

Usage Guidelines

The **show blocks** command helps you determine if the ASA is overloaded. This command lists preallocated system buffer utilization. A full memory condition is not a problem as long as traffic is moving through the ASA. You can use the **show conn** command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem.

You can also view this information using SNMP.

The information shown in a security context includes the system-wide information as well as context-specific information about the blocks in use and the high water mark for block usage.

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show blocks** command in single mode:

```
ciscoasa# show blocks
  SIZE    MAX    LOW    CNT   FAILED
     0    100     99    100      0
     4   1600   1598   1599      0
    80    400    398    399      0
   256   3600   3540   3542      0
  1550   4716   3177   3184      0
 16384     10     10     10      0
  2048   1000   1000   1000      0
```

Table 30: show blocks Fieldsshows each field description.

Table 30: show blocks Fields

Field	Description
SIZE	Size, in bytes, of the block pool. Each size represents a particular type.
0	Used by dupb blocks.
4	Duplicates existing blocks in applications such as DNS, ISAKMP, URL filtering, uauth, TFTP, and TCP modules. Also, this sized block can be used normally by code to send packets to drivers, etc.
80	Used in TCP intercept to generate acknowledgment packets and for failover hello messages.
256	Used for Stateful Failover updates, syslogging, and other TCP functions. These blocks are mainly used for Stateful Failover messages. The active ASA generates and sends packets to the standby ASA to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available blocks might drop to 0. This situation indicates that one or more connections were not updated to the standby ASA. The Stateful Failover protocol catches the missing translation or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the ASA is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the ASA is processing. Syslog messages sent out from the ASA also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the ASA configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.

Field	Description
1550	Used to store Ethernet packets for processing through the ASA. When a packet enters an ASA interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. The ASA determines whether the packet should be permitted or denied based on the security policy and processes the packet through to the output queue on the outbound interface. If the ASA is having trouble keeping up with the traffic load, the number of available blocks will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the ASA attempts to allocate more blocks. The maximum can be greater than 8192 for 1550-byte blocks if you issue this command. If no more blocks are available, the ASA drops the packet.
16384	Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543). See the description for 1550 for more information about Ethernet packets.
2048	Control or guided frames used for control updates.
MAX	Maximum number of blocks available for the specified byte block pool. The maximum number of blocks are carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the ASA can dynamically create more when needed. The maximum can be greater than 8192 for 1550-byte blocks if you issue this command.
LOW	Low-water mark. This number indicates the lowest number of this size blocks available since the ASA was powered up, or since the last clearing of the blocks (with the **clear blocks** command). A zero in the LOW column indicates a previous event where memory was full. **Note** To reset this value to MAX, you must reboot ASA.
CNT	Current number of blocks available for that specific size block pool. A zero in the CNT column means memory is full now.
FAILED	When the memory count for a block size is completely exhausted (LOW and CNT value is zero), the corresponding FAILED column is incremented with the number of allocation request for the same block size received thereafter. Eventually, when the memory space is freed, the current available blocks for allocation increments and the FAILED column value decreases. However, if CNT and FAILED values increase, it indicates an issue and must be resolved.

Examples

The following is sample output from the **show blocks all** command:

```
ciscoasa# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc not_specified
...
    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

Table 31: show blocks all Fields shows each field description.

Table 31: show blocks all Fields

Field	Description
Block	The block address.
allocd_by	The program address of the application that last used the block (0 if not used).
freed_by	The program address of the application that last released the block.
data size	The size of the application buffer/packet data that is inside the block.
alloccnt	The number of times this block has been used since the block came into existence.
dup_cnt	The current number of references to this block if used: 0 means 1 reference, 1 means 2 references.
oper	One of the four operations that was last performed on the block: alloc, get, put, or free.
location	The application that uses the block, or the program address of the application that last allocated the block (same as the allocd_by field).

Examples

The following is sample output from the **show blocks** command in a context. In multiple context mode, the output includes information on the number of blocks currently in use by the context (INUSE), and the high-water mark for blocks used by the context (HIGH).

```
ciscoasa/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

The following is sample output from the **show blocks queue history** command:

```
ciscoasa# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                 contexta
     15     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contextb
      1     1 put                                 contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contextb
      1     1 put                                 contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb
Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
```

```
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                 contexta
     15     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contextb
      1     1 put                                 contextc
...
```

The following is sample output from the **show blocks queue history detail** command:

```
ciscoasa# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                                 contexta
     15     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contextb
      1     1 put                                 contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contexta
      1     1 put                                 contextb
      1     1 put                                 contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...
total_count: total buffers in this class
```

The following is sample output from the **show blocks pool summary** command:

```
ciscoasa# show blocks pool 1550 summary
Class 3, size 1550
=================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000
```

```
=================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
=================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000
=================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

The following is sample output from the **show blocks exhaustion history list** command:

```
ciscoasa# show blocks exhaustion history list
1 Snapshot created at 18:01:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
2 Snapshot created at 18:02:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
3 Snapshot created at 18:03:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
4 Snapshot created at 18:04:03 UTC Feb 19 2014:
   Snapshot created due to 16384 blocks running out
```

Table 32: show blocks pool summary Fields shows each field description.

Table 32: show blocks pool summary Fields

Field	Description
total_count	The number of blocks for a given class.
miss_count	The number of blocks not reported in the specified category due to technical reasons.
Freed_pc	The program addresses of applications that released blocks in this class.
Alloc_pc	The program addresses of applications that allocated blocks in this class.
Queue	The queues to which valid blocks in this class belong.
valid_cnt	The number of blocks that are currently allocated.
invalid_cnt	The number of blocks that are not currently allocated.
Invalid Bad qtype	Either this queue has been freed and the contents are invalid or this queue was never initialized.
Valid tcp_usr_conn_inp	The queue is valid.

The following is sample output from the **show blocks depleted** command:

```
ciscoasa# show blocks depleted 8192

Block Class: 8,   Class Size: 8192,   Count: 100

1 Depletion created at 11:47:48 UTC Feb 17 2022

First Snapshot Details:

 Block             allocd_by          freed_by            alloccnt    dup_cnt  timestamp
  oper location

0x00007f117bd5f9c0 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd5d300 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd5ac40 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd58580 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd55ec0 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd53800 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd51140 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd4ea80 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd4c3c0 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd49d00 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd47640 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd44f80 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd428c0 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd40200 0x0000560e84d1236b 0x0000560e822144e4     1          0     246610
     alloc 0x0000560e84d1236b

0x00007f117bd3db40 0x0000560e84d1236b 0x0000560e822144e4     1          0     246620
     alloc 0x0000560e84d1236b

0x00007f117bd3b480 0x0000560e84d1236b 0x0000560e822144e4     1          0     246620
     alloc 0x0000560e84d1236b

<--- More --->

0x00007f117bc85a40 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
```

```
     alloc 0x0000560e84d1236b

0x00007f117bc83380 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc80cc0 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc7e600 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc7bf40 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc79880 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

<--- More --->

. . . . .
. . . . .

0x00007f117bc771c0 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc74b00 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc72440 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b

0x00007f117bc6fd80 0x0000560e84d1236b 0x0000560e822144e4     1          0     263390
     alloc 0x0000560e84d1236b
```

Related Commands

Command	Description
blocks	Increases the memory assigned to block diagnostics
clear blocks	Clears the system buffer statistics.
show conn	Shows active connections.

show bootvar

To show the boot file and configuration properties, use the **show bootvar** command in privileged EXEC mode.

show bootvar

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The BOOT variable specifies a list of bootable images on various devices. The CONFIG_FILE variable specifies the configuration file used during system initialization. Set these variables with the **boot system** command and **boot config** command, respectively.

Examples

The BOOT variable contains disk0:/f1_image, which is the image booted when the system reloads. The current value of BOOT is disk0:/f1_image; disk0:/f1_backupimage. This value means that the BOOT variable has been modified with the **boot system** command, but the running configuration has not been saved with the **write memory** command. When the running configuration is saved, the BOOT variable and current BOOT variable will both be disk0:/f1_image; disk0:/f1_backupimage. Assuming that the running configuration is saved, the boot loader will try to load the contents of the BOOT variable, starting with disk0:/f1image, but if that is not present or invalid, the boot loader will try to boot disk0:1/f1_backupimage.

The CONFIG_FILE variable points to the system startup configuration. In this example it is not set, so the startup configuration file is the default specified with the **boot config** command. The current CONFIG_FILE variable may be modified with the **boot config** command and saved with the **write memory** command.

The following is sample output from the **show bootvar** command:

```
ciscoasa# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
```

```
CONFIG_FILE variable =
Current CONFIG_FILE variable =
ciscoasa#
```

Related Commands

Command	Description
boot	Specifies the configuration file or image file used at startup.

show bridge-group

To show bridge group information such as interfaces assigned, MAC addresses, and IP addresses, use the **show bridge-group** command in privileged EXEC mode.

show bridge-group *bridge_group_number*

Syntax Description

bridge_group_number	Specifies the bridge group number as an integer between 1 and 100.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.
9.7(1)	We added support in routed mode for Integrated Routing and Bridging.

Examples

The following is sample output from the **show bridge-group** command with IPv4 addresses:

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    N/A
 Static mac-address entries: 0
 Dynamic mac-address entries: 2
```

The following is sample output from the **show bridge-group** command with IPv4 and IPv6 addresses:

```
ciscoasa# show bridge-group 1
 Interfaces: GigabitEthernet0/0.101, GigabitEthernet0/0.201
 Management System IP Address: 10.0.1.1 255.255.255.0
 Management Current IP Address: 10.0.1.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):
    2000:100::1, subnet is 2000:100::/64
    2000:101::1, subnet is 2000:101::/64
    2000:102::1, subnet is 2000:102::/64
```

```
Static mac-address entries: 0
Dynamic mac-address entries: 2
```

Related Commands

Command	Description
bridge-group	Groups transparent firewall interfaces into a bridge group.
clear configure interface bvi	Clears the bridge group interface configuration.
interface	Configures an interface.
interface bvi	Creates a bridge virtual interface.
ip address	Sets the management IP address for a bridge group.
show running-config interface bvi	Shows the bridge group interface configuration.

show call-home

To display the configured Call Home information, use the **show call-home** command in privileged EXEC mode.

[**cluster exec**] **show call-home** [**alert-group | detail | events | mail-server | status | profile** { *profile_name* | **all** } | **statistics**]

Syntax Description

alert-group	(Optional) Displays the available alert group.
cluster exec	(Optional) In a clustering environment, enables you to issue the **show call-home** command in one unit and run the command in all the other units at the same time.
detail	(Optional) Displays the Call Home configuration in detail.
events	(Optional) Displays current detected events.
mail-server status	(Optional) Displays the Call Home mail server status information.
profile *profile _name* **all**	(Optional) Displays configuration information for all existing profiles.
statistics	(Optional) Displays the Call Home statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added.
9.1(3)	A new type of Smart Call Home message has been added to include the output of the **show cluster history** command and **show cluster info** command.

Examples

The following is sample output from the show call-home command and displays the configured Call Home settings:

```
ciscoasa# show call-homeCurrent Smart Call-Home settings:Smart Call-Home feature : enableSmart
```

```
 Call-Home message's from address: from@example.comSmart Call-Home message's reply-to
address: reply-to@example.comcontact person's email address: example@example.comcontact
person's phone: 111-222-3333street address: 1234 Any Street, Any city, Any state,
12345customer ID: ExampleCorpcontract ID: X123456789site ID: SantaClaraMail-server[1]:
Address: smtp.example.com Priority: 1Mail-server[2]: Address: 192.168.0.1 Priority:
10Rate-limit: 60 message(s) per minute
Available alert groups:Keyword                  State
------------------------ -------
Syslog Enable
diagnostic Enableenvironmental Enableinventory Enableconfiguration Enablefirewall
Enabletroubleshooting Enablereport Enable
Profiles:Profile Name: CiscoTAC-1Profile Name: prof1Profile Name: prof2
```

The following is sample output from the show call-home detail command and displays detailed Call Home configuration information:

```
ciscoasa# show call-home detailDescription: Show smart call-home configuration in
detail.Supported Modes: single mode and system context in multi mode,
routed/transparent.Output:
Current Smart Call-Home settings:Smart Call-Home feature: enableSmart Call-Home message's
from address: from@example.example.comSmart Call-Home message's reply-to address:
reply-to@example.example.comcontact person's email address: abc@example.comcontact person's
 phone: 111-222-3333street address: 1234 Any Street, Any city, Any state, 12345customer ID:
 111111contract ID: 123123site ID: SantaClaraMail-server[1]: Address: example.example.com
Priority: 1Mail-server[2]: Address: example.example.com Priority: 10Rate-limit: 60 message(s)
 per minute
Available alert groups:Keyword State------------------------ -------syslog Enablediagnostic
 Enableenvironmental Enableinventory Enableconfiguration Enablefirewall Enabletroubleshooting
 Enablereport Enable
Profiles:
Profile Name: CiscoTAC-1Profile status: ACTIVE Preferred Message Format: xmlMessage Size
Limit: 3145728 BytesEmail address(es): anstage@cisco.comHTTP address(es):
https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity------------------------ ------------inventory n/a
Profile Name: prof1Profile status: ACTIVE Preferred Message Format: xmlMessage Size Limit:
 3145728 BytesEmail address(es): example@example.comHTTP address(es):
https://kafan-lnx-01.cisco.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity------------------------ ------------configuration n/ainventory n/a
Profile Name: prof2Profile status: ACTIVE Preferred Message Format: short-textMessage Size
 Limit: 1048576 BytesEmail address(es): example@example.comHTTP address(es):
https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity------------------------ ------------configuration n/ainventory n/a
```

The following is sample output from the show call-home events command and displays available Call Home events:

```
ciscoasa# show call-home eventsDescription: Show current detected events.Supported Modes:
single mode and system context in multi mode, routed/transparent.Output:Active event
list:Event client alert-group severity active
(sec)--------------------------------------------------------------------Configuration
Client configuration none 5Inventory inventory none 15
```

The following is sample output from the show call-home mail-server status command and displays available Call Home mail-server status:

```
ciscoasa# show call-home mail-server statusDescription: Show smart call-home configuration,
 status, and statistics.Supported Modes: single mode and system context in multi mode,
routed/transparent.Output:Mail-server[1]: Address: example.example.com Priority: 1
[Available]Mail-server[2]: Address: example.example.com Priority: 10 [Not Available]
```

The following is sample output from the show call-home alert-group command and displays the available alert groups:

```
ciscoasa# show call-home alert-groupDescription: Show smart call-home alert-group
states.Supported Modes: single mode and system context in multi mode,
routed/transparent.Output:Available alert groups:Keyword State------------------------
-------syslog Enablediagnostic Enableenvironmental Enableinventory Enableconfiguration
Enablefirewall Enabletroubleshooting Enablereport Enable
```

The following is sample output from the show call-home profile profile-name | all command and displays information for all predefined and user-defined profiles:

```
ciscoasa# show call-home profile {profile-name
 | all}Description: Show smart call-home profile configuration.Supported Modes: single mode
 and system context in multi mode, routed/transparent.Output:Profiles:
Profile Name: CiscoTAC-1Profile status: ACTIVE Preferred Message Format: xmlMessage Size
Limit: 3145728 BytesEmail address(es): anstage@cisco.comHTTP address(es):
https://tools.cisco.com/its/service/oddce/services/DDCEService
Periodic inventory message is scheduled monthly at 01:00
Alert-group Severity------------------------ ------------inventory n/a
Profile Name: prof1Profile status: ACTIVE Preferred Message Format: xmlMessage Size Limit:
 3145728 BytesEmail address(es): example@example.comHTTP address(es):
https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled daily at 01:00
Periodic inventory message is scheduled every 60 minutes
Alert-group Severity------------------------ ------------configuration n/ainventory n/a
Profile Name: prof2Profile status: ACTIVE Preferred Message Format: short-textMessage Size
 Limit: 1048576 BytesEmail address(es): example@example.comHTTP address(es):
https://example.example.com:8443/sch/sch.jsp
Periodic configuration message is scheduled every 1 minutes
Periodic inventory message is scheduled every 1 minutes
Alert-group Severity------------------------ ------------configuration n/ainventory n/a
```

The following is sample output from the show call-home statistics command and displays the call-home statistics:

```
ciscoasa# show call-home statisticsDescription: Show smart call-home statistics.Supported
Modes: single mode and system context in multi mode, routed/transparent.Output:Message Types
 Total Email HTTP-------------------- ---------------- ---------------- ----------------Total
 Success 0 0 0
Total In-Queue 0 0 0
Total Dropped 5 4 1Tx Failed 5 4 1inventory 3 2 1configuration 2 2 0
Event Types Total-------------------- ----------------Total Detected 2inventory 1configuration
 1
Total In-Queue 0
Total Dropped 0
Last call-home message sent time: 2009-06-17 14:22:09 GMT-07:00
```

The following is sample output from the show call-home status command and displays the call-home status:

```
ciscoasa# show call-home mail-server status
Description: Show smart call-home configuration, status, and statistics.Supported Modes:
single mode and system context in multi mode, routed/transparent.Output:Mail-server[1]:
Address: kafan-lnx-01.cisco.com Priority: 1 [Available]Mail-server[2]: Address:
kafan-lnx-02.cisco.com Priority: 10 [Not Available]37. ciscoasa# show call-home events
Description: Show current detected events.Supported Modes: single mode and system context
in multi mode, routed/transparent.Output:Active event list:Event client alert-group severity
```

```
 active (sec)-----------------------------------------------------------------Configuration
 Client configuration none 5Inventory inventory none 15
```

The following is sample output from the **cluster exec show call-home statistics** command and displays call-home statistics for a cluster:

```
ciscoasa(config)# cluster exec show call-home statistics
A(LOCAL):*************************************************************
Message Types           Total            Email            HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                3                3                0
                test                3                3                0
 Total In-Delivering                0                0                0
      Total In-Queue                0                0                0
Total Dropped                       8                8                0
           Tx Failed                8                8                0
       configuration                2                2                0
                test                6                6                0
Event Types             Total
--------------------   ----------------
      Total Detected               10
       configuration                1
                test                9
 Total In-Processing                0
      Total In-Queue                0
Total Dropped                       0
Last call-home message sent time: 2013-04-15 05:37:16 GMT+00:00
B:*******************************************************************
Message Types           Total            Email            HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                1                1                0
                test                1                1                0
 Total In-Delivering                0                0                0
      Total In-Queue                0                0                0
Total Dropped                       2                2                0
           Tx Failed                2                2                0
       configuration                2                2                0
Event Types             Total
--------------------   ----------------
      Total Detected                2
       configuration                1
                test                1
 Total In-Processing                0
      Total In-Queue                0
Total Dropped                       0
Last call-home message sent time: 2013-04-15 05:36:16 GMT+00:00
C:*******************************************************************
Message Types           Total            Email            HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                0                0                0
 Total In-Delivering                0                0                0
      Total In-Queue                0                0                0
Total Dropped                       2                2                0
           Tx Failed                2                2                0
       configuration                2                2                0
Event Types             Total
--------------------   ----------------
      Total Detected                1
       configuration                1
 Total In-Processing                0
      Total In-Queue                0
Total Dropped                       0
Last call-home message sent time: n/a
```

```
D:*******************************************************************
Message Types           Total            Email            HTTP
--------------------   ---------------- ---------------- ----------------
       Total Success                  1                1                0
                test                  1                1                0
 Total In-Delivering                  0                0                0
      Total In-Queue                  0                0                0
Total Dropped                         2                2                0
           Tx Failed                  2                2                0
       configuration                  2                2                0
Event Types             Total
--------------------   ----------------
      Total Detected                  2
       configuration                  1
                test                  1
 Total In-Processing                  0
      Total In-Queue                  0
Total Dropped                         0
Last call-home message sent time: 2013-04-15 05:35:34 GMT+00:00
ciscoasa(config)#
```

Related Commands

Command	Description
call-home	Enters call home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.

show call-home registered-module status

To display the registered module status, use the **show call-home** registered-module status command in privileged EXEC mode.

show call-home registered-module status [**all**]

Note The [**all**] option is only valid in system context mode.

Syntax Description

al	Displays module status based on the device, not per context. In multiple context mode, if a module is enabled in at least one context, it is displayed as enabled if the "**all**" option is included.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(2)	This command was added.

Examples

The following example displays the **show call-home** registered-module status **all** output:

```
Output:
Module Name  Status
---------------------------------------- --------------------Smart Call-Home enabledFailover
 Standby/Active
```

Related Commands

Command	Description
call-home	Enters call-home configuration mode.
call-home send alert-group	Sends a specific alert group message.
service call-home	Enables or disables Call Home.

show capture

To display the capture configuration when no options are specified, use the **show capture** command in privileged EXEC mode.

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*] [**trace**]

Syntax Description

access-list *access_list_name*	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification .
capture_name	(Optional) Specifies the name of the packet capture.
cluster exec	(Optional) In a clustering environment, enables you to issue the **show capture** command in one unit and run the command in all the other units at the same time.
count *number*	(Optional) Displays the number of packets specified data.
decode	This option is useful when a capture of type isakmp is applied to an interface. All ISAKMP data flowing through that interface will be captured after decryption and shown with more information after decoding the fields.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link.
packet-number *number*	Starts the display at the specified packet number.
trace	Displays extended trace information for each packet.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	Detailed information in the output for IDS was added.

Release	Modification
9.0(1)	The **cluster exec** option was added.
9.2(1)	The **vpn-user** domain name was changed to **filter-aaa** in the output.
9.3(1)	Output for SGT plus Ethernet Tagging was added.
9.10(1)	IP decode support for GRE and IPinIP encapsulation was added.
9.13(1)	The show capture for asp-drop capture type was enhanced to include location details of the drop.
9.20(2)	The show capture detail for the physical port displays the drop configuration (disable or mac-filter).

Usage Guidelines

If you specify the *capture_name* , then the capture buffer contents for that capture are displayed.

The **dump** keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. Typically, this command supports IP decode for the ICMP, UDP, and TCP protocols. From version 9.10(1), this command is enhanced to support the display of the IP decode output for GRE and IPinIP encapsulation on ICMP, UDP, and TCP.

In Table 33: Packet Capture Output Formats, the bracketed output is displayed when you specify the **detail** keyword.

Table 33: Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info* *encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type* *arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type* *icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr* . *src-port* *dest-addr* . *dst-port* : [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr* . *src-port* d *est-addr* . *dst-port* : *tcp-flags* [header-check] [checksum-info] *sequence-number* *ack-number* *tcp-window* *urgent-info* *tcp-options*

Packet Type	Capture Output Format
IP/GRE	**ICMP encapsulated with GRE:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: gre:* [gre-flags] *ip-source > ip-destination: icmp: icmp-type icmp-code* [checksum-failure] **UDP encapsulated with GRE:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: gre:* [gre-flags] *src-addr.src-port dest-addr.dst-port:* [checksum-info] *udp payload-len* **TCP encapsulated with GRE:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: gre:* [gre-flags] *src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/IPinIP	**ICMP encapsulated with IPinIP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: ipip-proto-4: ip-source > ip-destination: icmp: icmp-type icmp-code* [checksum-failure] **UDP encapsulated with IPinIP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: ipip-proto-4: src-addr.src-port dest-addr.dst-port:* [checksum-info] *udp payload-len* **TCP encapsulated with IPinIP:** *HH:MM:SS.ms* [ether-hdr] *carrier-ip-source> carrier-ip-destination: ipip-proto-4: src-addr.src-port dest-addr.dst-port: tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr* : *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr* : *hex-dump*

Usage Guidelines

If the ASA receives packets with an incorrectly formatted TCP header and drops them because of the ASP drop reason *invalid-tcp-hdr-length* , the **show capture** command output on the interface where those packets are received does not show those packets.

From version 9.13(1), to facilitate troubleshooting, the show capture output is enhanced to include the drop location information when showing the capture type of asp-drop. While troubleshooting using ASP drop counters, the exact location of the drop is unknown, especially when the same ASP drop reason is used in many different places. This information is critical in finding root cause of the drop. With this enhancement, the ASP drop details such as the build target, ASA release number, hardware model, and ASLR memory text region (to facilitate the decode of drop location) are shown.

Examples

This example shows how to display the capture configuration:

```
ciscoasa(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```
ciscoasa(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

The following example shows how to display the packets that are captured on a single unit in a clustering environment:

```
ciscoasa(config)# show capture
capture 1 cluster type raw-data interface primary interface cluster [Buffer Full - 524187
bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
```

The following example shows how to display the packets that are captured on all units in a clustering environment:

```
ciscoasa(config)# cluster exec
            show capture
mycapture (LOCAL):---------------------------------------------------------
capture 1 type raw-data interface primary [Buffer Full - 524187 bytes]
capture 2 type raw-data interface cluster [Capturing - 232354 bytes]
yourcapture:---------------------------------------------------------------
capture 1 type raw-data interface primary [Capturing - 191484 bytes]
capture 2 type raw-data interface cluster [Capturing - 532354 bytes]
```

The following example shows the packets that are captured on the cluster control link in a clustering environment after the following commands are entered:

```
ciscoasa (config)# capture a interface cluster
ciscoasa (config)# capture cp interface cluster match udp any eq 49495 any
ciscoasa (config)# capture cp interface cluster match udp any any eq 49495
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet 0/0
ciscoasa(config)# show capture
capture a type raw-data interface cluster [Capturing - 970 bytes]
capture cp type raw-data interface cluster [Capturing - 26236 bytes]
  match udp any eq 49495 any
capture dp type raw-data access-list cc1 interface cluster [Capturing - 4545230 bytes]
capture lacp type lacp interface gigabitEthernet0/0 [Capturing - 140 bytes]
```

The following example shows the packets that are captured when SGT plus Ethernet tagging has been enabled on an interface:

```
ciscoasa(config)# show capture my-inside-capture
1: 11:34:42.931012 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
2: 11:34:42.931470 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
3: 11:34:43.932553 INLINE-TAG 36 10.0.101.22 > 11.0.101.100: icmp: echo request
4: 11.34.43.933164 INLINE-TAG 48 11.0.101.100 > 10.0.101.22: icmp: echo reply
```

When SGT plus Ethernet tagging has been enabled on an interface, the interface can still receive tagged or untagged packets. The example shown is for tagged packets, which have INLINE-TAG 36 in the output. When the same interface receives untagged packets, the output remains unchanged (that is, no "INLINE-TAG 36" entry is included in the output).

The following example shows the GRE, IPinIP, and other packets that are generated by packet tracer and the subsequent capture output on interface inside:

GRE packets:

```
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside gre ipv4 31.1.1.6 32.1.1.6 icmp 1.1.1.1 8 0 2.2.2.2
```

IPinIP Packets:

```
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside ipip 31.1.1.6 32.1.1.6 icmp 1.1.1.1 8 0 2.2.2.2
```

Regular tcp/udp/icmp packets:

```
packet-tracer input inside tcp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside udp 1.1.1.1 1234 2.2.2.2 80
packet-tracer input inside icmp 1.1.1.1 8 0 2.2.2.2

ciscoasa(config)# show capture inside
12:10:37.523746       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1.1234 > 2.2.2.2.80: S
2145492151:2145492151(0) win 8192
12:10:37.623624       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:10:37.714471       31.1.1.6 > 32.1.1.6: gre: 1.1.1.1 > 2.2.2.2 icmp: echo request
12:10:37.806690       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1.1234 > 2.2.2.2.80: S
1501131661:1501131661(0) win 8192
12:10:37.897673       31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1.1234 > 2.2.2.2.80:  udp 0

12:10:41.974604      31.1.1.6 > 32.1.1.6: ipip-proto-4: 1.1.1.1 > 2.2.2.2 icmp: echo request
12:16:14.957225       1.1.1.1.1234 > 2.2.2.2.80: S 2091733697:2091733697(0) win 8192
12:16:15.023909       1.1.1.1.1234 > 2.2.2.2.80:  udp 0
12:16:15.090449       1.1.1.1 > 2.2.2.2 icmp: echo request
```

Note The GRE and IPinIP packets are decoded using the TCP/UDP/ICMP decode functionality to display the inner packet.

The following example shows the enhancement made to the output of this command. The drop location program counter or current instruction (which is later decoded), the build target, ASA release number, hardware model, and ASLR memory text region are captured and displayed to facilitate the decode of drop location:

```
ciscoasa(config)# capture gtp_drop type asp-drop inspect-gtp
ciscoasa(config)# show capture gtp_drop [trace]
Target:         SSP
Hardware:   FPR4K-SM-12
Cisco Adaptive Security Appliance Software Version 9.13.1
ASLR enabled, text region 55cd421df000-55cd47530ea9
1 packets captured

1: 15:55:58.522983       192.168.108.12.41245 > 171.70.168.183.2123:  udp 27 Drop-reason:
(inspect-gtp) GTP inspection, Drop-location: frame 0x000055cd43db4019 flow (NA)/NA
```

```
ciscoasa(config)# show capture gtp_drop trace detail
Target:         SSP
Hardware:   FPR4K-SM-12
Cisco Adaptive Security Appliance Software Version 9.13.1
ASLR enabled, text region 55cd421df000-55cd47530ea9
1 packets captured

1: 15:55:58.522983 0050.56b0.bd99 5057.a884.2beb 0x0800 Length: 69
192.168.108.12.41245 > 171.70.168.183.2123:  [udp sum ok] udp 27 (ttl 64, id 53384)
Drop-reason: (inspect-gtp) GTP inspection, Drop-location: frame 0x000055cd43db4019 flow
(NA)/NA
```

The following example shows the packet captured with the mac-filter drop enabled:

```
ciscoasa(config)# show capture test detail
Packet Capture info
Name:test
Session: 3
Admin State: disabled
OperState:down
OperState Reason: Session_Admin_Shut
Config Success:yes
Config Fail Reason:
Append Flag: overwrite
Session Mem Usage: 256
Session PcapSnap Len: 1518
Error Code:0
Drop Count:0
Total Physical ports involved in Packet Capture: 1

Physical port:
Slot Id: 1
Port Id: 1
Pcapfile:/mnt/disk0/packet-capture/sess-3-test-ethernet-1-1-0.
pcapPcapsize:0
Drop:mac-filter
Filter:test-1-1
Packet Capture Filter Info
Name:test-1-1
Protocol:0
Ivlan: 0
Ovlan: 3178
SrcIp:0.0.0.0
DestIp: 0.0.0.0
SrcIpv6:::
DestIpv6: ::
SrcMAC: 00:00:00:00:00:00
DestMAC:00:00:00:00:00:00
SrcPort:0
DestPort: 0
Ethertype: 0
Total Physical breakout ports involved in Packet Capture: 0
0 packet captured on disk using switch capture
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
copy capture	Copies a capture file to a server.

show chardrop

To display the count of characters dropped from the serial console, use the **show chardrop** command in privileged EXEC mode.

show chardrop

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following is sample output from the **show chardrop** command:

```
ciscoasa# show chardrop
Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0
```

Related Commands

Command	Description
show running-config	Shows the current operating configuration.

show checkheaps

To show the checkheaps statistics, use the **show checkheaps** command in privileged EXEC mode. Checkheaps is a periodic process that verifies the sanity of the heap memory buffers (dynamic memory is allocated from the system heap memory region) and the integrity of the code region.

show checkheaps

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show checkheaps** command:

```
ciscoasa# show checkheaps
Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run      : 42 secs
Duration of last run             : 0 millisecs
Number of buffers created        : 8082
Number of buffers allocated      : 7808
Number of buffers free           : 274
Total memory in use              : 43570344 bytes
Total memory in free buffers     : 87000 bytes
Total number of runs             : 310
```

Related Commands

Command	Description
checkheaps	Sets the checkheap verification intervals.

show checksum

To display the configuration checksum, use the **show checksum** command in privileged EXEC mode.

show checksum

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The show checksum command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This checksum is calculated only when you store the configuration in flash memory.

If a dot (".") appears before the checksum in the show config or show checksum command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the ASA flash partition). The "." shows that the ASA is preoccupied with the operation but is not "hung up." This message is similar to a "system processing, please wait" message.

Examples

This example shows how to display the configuration or the checksum:

```
ciscoasa(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

To display the chunk statistics, use the **show chunkstat** command in privileged EXEC mode.

show chunkstat

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The output of this command is primarily for internal development usage, and it is not meaningful for customers.

Examples

This example shows how to display the chunk statistics:

```
ciscoasa# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings destroyed
 34
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24, end
 @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
show cpu	Displays the CPU utilization information.

show class

To show the contexts assigned to a class, use the **show class** command in privileged EXEC mode.

show class *name*

Syntax Description

name	Specifies the name as a string up to 20 characters long. To show the default class, enter **default** for the name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following is sample output from the **show class default** command:

```
ciscoasa# show class default
Class Name           Members    ID   Flags
default                All       1    0001
```

Related Commands

Command	Description
class	Configures a resource class.
clear configure class	Clears the class configuration.
context	Configures a security context.
limit-resource	Sets the resource limit for a class.
member	Assigns a context to a resource class.

show clns

To show Connectionless-mode Network Service (CLNS) information for IS-IS, use the **show clns** command in privileged EXEC mode.

show clns { **filter-set | interface** [*interface_name*] | **is-neighbors** [*interface_name*] [**detail**] | **neighbors** [**areas**] [*interface_name*] [**detail**] | **protocol** [*domain*] | **traffic** [**since** { **bootup | show** }] }

Syntax Description

areas	(Optional) Shows CLNS multiarea adjacencies.
bootup	Shows CLNS protocol statistics since bootup.
detail	(Optional) Shows the areas associated with the intermediate systems. Otherwise, a summary display is provided.
domain	(Optional) Shows routing protocol process information for a CLNS domain.
filter-set	Shows CLNS filter sets.
interface	Shows CLNS interface status and configuration.
interface_name	(Optional) Specifies the interface name.
is-neighbors	Shows IS neighbor adjacencies. Neighbor entries are sorted according to the area in which they are located.
neighbors	Displays end system (ES), intermediate system (IS), and multitopology Integrated Intermediate System-to-Intermediate System (M-ISIS) neighbors
protocol	Shows CLNS routing protocol process information. There will always be at least two routing processes, a Level 1 and a Level 2, and there can be more.
show	Shows CLNS protocol statistics since the last time you used this **show** command.
since	(Optional) Shows CLNS protocol statistics since either bootup or the last time you used this **show** command.
traffic	Lists the CLNS packets that this router has seen.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

This command shows CLNS information for IS-IS.

Examples

The following display assumes filter sets have been defined with the following commands:

```
ciscoasa(config)# clns filter-set US-OR-NORDUNET 47.0005..
.
ciscoasa(config)# clns filter-set US-OR-NORDUNET 47.0023...

ciscoasa(config)# clns filter-set LOCAL 49.0003...
```

The following is a sample output from the **show clns filter-set** command:

```
ciscoasa# show clns filter-set
CLNS filter set US-OR-NORDUNET
      permit 47.0005...
      permit 47.0023...
CLNS filter set LOCAL
      permit 49.0003...
```

The following is sample output from the **show clns interface** command that includes information for Token Ring and serial interfaces:

```
ciscoasa# show clns interface
GigabitEthernet0/1 is up, line protocol is up
  Checksums enabled, MTU 1500
  ERPDUs enabled, min. interval 10 msec.
  DEC compatibility mode OFF for this interface
  Next ESH/ISH in 0 seconds
  Routing Protocol: IS-IS
    Circuit Type: level-1-2
    Interface number 0x0, local circuit ID 0x1
    Level-1 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-1 IPv6 Metric: 10
    Number of active level-1 adjacencies: 3
    Level-2 Metric: 10, Priority: 64, Circuit ID: c2.01
    DR ID: c2.01
    Level-2 IPv6 Metric: 10
    Number of active level-2 adjacencies: 3
    Next IS-IS LAN Level-1 Hello in 1 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
```

Table 34: show clns interface fields

Field	Description
GigabitEthernet0/1 is up, line protocol is up	Shown to be up, and the line protocol is up.
Checksums enabled	Can be enabled or disabled.
MTU	The number following maximum transmission unit (MTU) is the maximum transmission size for a packet on this interface.
ERPDUs	Displays information about the generation of error protocol data units (ERPDUs). They can be either enabled or disabled. If they are enabled, they are sent out no more frequently than the specified interval.
RDPDUs	Provides information about the generation of redirect protocol data units (RDPDUs). They can be either enabled or disabled. If they are enabled, they are sent out no more frequently than the specified interval. If the address mask is enabled, redirects are sent out with an address mask.
Congestion Experienced	Tells when CLNS will turn on the congestion experienced bit. The default is to turn this bit on when there are more than four packets in a queue.
DEC compatibility mode	Indicates whether Digital Equipment Corporation (DEC) compatibility has been enabled.
Next ESH/ISH	Displays when the next end system (ES) hello or intermediate system (IS) hello will be sent on this interface.
Routing Protocol	Lists the areas that this interface is in. In most cases, an interface will be in only one area.
Circuit Type	Indicates whether the interface has been configured for local routing (level 1), area routing (level 2), or local and area routing (level 1-2).
Interface number, local circuit ID; Level-1 Metric; DR ID; Level-1 IPv6 Metric; Number of active level-1 adjacencies; Level-2 Metric; DR ID; Level-2 IPv6 Metric; Number of active level-2 adjacencies; Next IS-IS LAN Level-1; Next IS-IS LAN Level-2	Last series of fields displays information pertaining to Intermediate System-to-Intermediate System (IS-IS). For IS-IS, the Level 1 and Level 2 metrics, priorities, circuit IDs, and number of active Level 1 and Level 2 adjacencies are specified.
BFD enabled	BFD has been enabled on the interface.

The following is sample output from the **show clns is-neighbors** command:

```
ciscoasa# show clns is-neighbors
System Id      Interface   State  Type Priority  Circuit Id         Format
```

```
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
```

Table 35: show clns is-neighbors Fields

Field	Description
System Id	Identification value of the system.
Interface	Interface on which the router was discovered.
State	Adjacency state. Up and Init are the states. See the show clns neighbors description.
Type	L1, L2, and L1L2 type adjacencies. See the **show clns neighbors** description.
Priority	IS-IS priority that the respective neighbor is advertising. The highest priority neighbor is elected the designated IS-IS router for the interface.
Circuit Id	Neighbor's idea of what the designated IS-IS router is for the interface.
Format	Indicates if the neighbor is either a Phase V (OSI) adjacency or Phase IV (DECnet) adjacency.

The following is sample output from the **show clns is-neighbors detail** command:

```
ciscoasa# show clns is-neighbors detail
System Id      Interface   State  Type Priority  Circuit Id         Format
CSR7001        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 00:12:49
  NSF capable
  Interface name: inside
CSR7002        inside      Up     L1L2 64/64    ciscoasa.01         Phase V
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 00:12:50
  NSF capable
  Interface name: inside
```

The following is sample output from the **show clns neighbors detail** command:

```
ciscoasa# show clns neighbors detail
System Id      Interface   SNPA                State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44      Up          26   L1L2
  Area Address(es): 49.0001
  IP Address(es):  1.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
CSR7002        inside      000c.2906.491c      Up          27   L1L2
  Area Address(es): 49.0001
  IP Address(es):  20.3.3.3*
  Uptime: 01:16:33
  NSF capable
  Interface name: inside
```

The following is sample output from the **show clns neighbors** command:

```
ciscoasa# show clns neighbors
```

```
System Id      Interface   SNPA              State  Holdtime  Type Protocol
CSR7001        inside      000c.2921.ff44    Up           29   L1L2
CSR7002        inside      000c.2906.491c    Up           27   L1L2
```

Table 36: show clns neighbors Fields

Field	Description
System Id	Six-byte value that identifies a system in an area.
Interface	Interface name from which the system was learned.
SNPA	Subnetwork Point of Attachment. This is the data-link address.
State	State of the ES, IS, or M-ISIS. • Init—System is an IS and is waiting for an IS-IS hello message. IS-IS regards the neighbor as not adjacent. • Up—Believes the ES or IS is reachable.
Holdtime	Number of seconds before this adjacency entry times out.
Type	The adjacency type. Possible values are as follows: • ES—End-system adjacency either discovered via the ES-IS protocol or statically configured. • IS—Router adjacency either discovered via the ES-IS protocol or statically configured. • M-ISIS—Router adjacency discovered via the multitopology IS-IS protocol. • L1—Router adjacency for Level 1 routing only. • L1L2—Router adjacency for Level 1 and Level 2 routing. • L2—Router adjacency for Level 2 only.
Protocol	Protocol through which the adjacency was learned. Valid protocol sources are ES-IS, IS-IS, ISO IGRP, Static, DECnet, and M-ISIS.

The following is sample output from the **show clns protocol** command:

```
ciscoasa# show clns protocol
IS-IS Router
  System Id: 0050.0500.5008.00  IS-Type: level-1-2
  Manual area address(es):
        49.0001
  Routing for area address(es):
        49.0001
  Interfaces supported by IS-IS:
        outside - IP
  Redistribute:
    static (on by default)
  Distance for L2 CLNS routes: 110
  RRR level: none
  Generate narrow metrics: level-1-2
  Accept narrow metrics:   level-1-2
  Generate wide metrics:   none
  Accept wide metrics:     none
```

The following is sample output from the **show clns traffic** command:

```
ciscoasa# show clns traffic
CLNS:  Time since last clear: never
CLNS & ESIS Output: 0, Input: 8829
CLNS Local: 0, Forward: 0
CLNS Discards:
  Hdr Syntax: 0, Checksum: 0, Lifetime: 0, Output cngstn: 0
  No Route: 0, Discard Route: 0, Dst Unreachable 0, Encaps. Failed: 0
  NLP Unknown: 0, Not an IS: 0
CLNS Options: Packets 0, total 0 , bad 0, GQOS 0, cngstn exprncd 0
CLNS Segments:  Segmented: 0, Failed: 0
CLNS Broadcasts: sent: 0, rcvd: 0
Echos: Rcvd 0 requests, 0 replies
      Sent 0 requests, 0 replies
ESIS(sent/rcvd): ESHs: 0/0, ISHs: 0/0, RDs: 0/0, QCF: 0/0
Tunneling (sent/rcvd): IP: 0/0, IPv6: 0/0
Tunneling dropped (rcvd) IP/IPV6:  0
ISO-IGRP: Querys (sent/rcvd): 0/0 Updates (sent/rcvd): 0/0
ISO-IGRP: Router Hellos: (sent/rcvd): 0/0
ISO-IGRP Syntax Errors: 0
IS-IS: Time since last clear: never
IS-IS: Level-1 Hellos (sent/rcvd): 1928/1287
IS-IS: Level-2 Hellos (sent/rcvd): 1918/1283
IS-IS: PTP Hellos     (sent/rcvd): 0/0
IS-IS: Level-1 LSPs sourced (new/refresh): 7/13
IS-IS: Level-2 LSPs sourced (new/refresh): 7/14
IS-IS: Level-1 LSPs flooded (sent/rcvd): 97/2675
IS-IS: Level-2 LSPs flooded (sent/rcvd): 73/2628
IS-IS: LSP Retransmissions: 0
IS-IS: Level-1 CSNPs (sent/rcvd): 642/0
IS-IS: Level-2 CSNPs (sent/rcvd): 639/0
IS-IS: Level-1 PSNPs (sent/rcvd): 0/554
IS-IS: Level-2 PSNPs (sent/rcvd): 0/390
IS-IS: Level-1 DR Elections: 1
IS-IS: Level-2 DR Elections: 1
IS-IS: Level-1 SPF Calculations: 9
IS-IS: Level-2 SPF Calculations: 8
IS-IS: Level-1 Partial Route Calculations: 0
IS-IS: Level-2 Partial Route Calculations: 0
IS-IS: LSP checksum errors received: 0
IS-IS: Update process queue depth: 0/200
IS-IS: Update process packets dropped: 0
```

Table 37: show clns traffic Fields

Field	Description
CLNS & ESIS Output	Total number of packets that this router has sent.
Input	Total number of packets that this router has received.
CLNS Local	Lists the number of packets that were generated by this router.
Forward	Lists the number of packets that this router has forwarded.
CLNS Discards	Lists the packets that CLNS has discarded, along with the reason for the discard.
CLNS Options	Lists the options seen in CLNS packets.

Field	Description
CLNS Segments	Lists the number of packets segmented and the number of failures that occurred because a packet could not be segmented.
CLNS Broadcasts	Lists the number of CLNS broadcasts sent and received.
Echos	Lists the number of echo request packets and echo reply packets received. The line following this field lists the number of echo request packets and echo reply packets sent.
ESIS (sent/rcvd)	Lists the number of End System Hello (ESH), Intermediate System Hello (ISH), and redirects sent and received.
ISO IGRP	Lists the number of ISO Interior Gateway Routing Protocol (IGRP) queries and updates sent and received.
Router Hellos	Lists the number of ISO IGRP router hello packets sent and received.
IS-IS: Level-1 hellos (sent/rcvd)	Lists the number of Level 1 IS-IS hello packets sent and received.
IS-IS: Level-2 hellos (sent/rcvd)	Lists the number of Level 2 IS-IS hello packets sent and received.
IS-IS: PTP hellos (sent/rcvd)	Lists the number of point-to-point IS-IS hello packets sent and received over serial links.
IS-IS: Level-1 LSPs (sent/rcvd)	Lists the number of Level 1 link-state Protocol Data Unit (PDUs) sent and received.
IS-IS: Level-2 LSPs (sent/rcvd)	Lists the number of Level 2 link-state PDUs sent and received.
IS-IS: Level-1 CSNPs (sent/rcvd)	Lists the number of Level 1 Complete Sequence Number Packets (CSNP) sent and received.
IS-IS: Level-2 CSNPs (sent/rcvd)	Lists the number of Level 2 CSNPs sent and received.
IS-IS: Level-1 PSNPs (sent/rcvd)	Lists the number of Level 1 Partial Sequence Number Packets (PSNP) sent and received.
IS-IS: Level-2 PSNPs (sent/rcvd)	Lists the number of Level 2 PSNPs sent and received.
IS-IS: Level-1 DR Elections	Lists the number of times Level 1 designated router election occurred.
IS-IS: Level-2 DR Elections	Lists the number of times Level 2 designated router election occurred.
IS-IS: Level-1 SPF Calculations	Lists the number of times the Level 1 shortest-path-first (SPF) tree was computed.
IS-IS: Level-2 SPF Calculations	Lists the number of times the Level 2 SPF tree was computed.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.

Command	Description
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.

Command	Description
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show clock

To view the time on the ASA, use the **show clock** command in user EXEC mode.

show clock [**detail**]

Syntax Description

detail	(Optional) Indicates the clock source (NTP or user configuration) and the current summer-time setting (if any).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show clock** command:

```
ciscoasa# show clock
12:35:45.205 EDT Tue Jul 27 2004
```

The following is sample output from the **show clock detail** command:

```
ciscoasa# show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

Related Commands

Command	Description
clock set	Manually sets the clock on the ASA.
clock summer-time	Sets the date range to show daylight saving time.
clock timezone	Sets the time zone.
ntp server	Identifies an NTP server.

Command	Description
show ntp status	Shows the status of the NTP association.

show cluster

To view aggregated data for the entire cluster or other information, use the **show cluster** command in privileged EXEC mode.

show cluster [**chassis**] { **access-list** [*acl_name*] | **conn** [**count**] | **context** [*context_name*] | **cpu** [**usage**] **interface-mode** | **memory** | **resource** | **service-policy** | **traffic** | **xlate count** }

Syntax Description

access-list [*acl_name*]	Shows hit counters for access policies. To see the counters for a specific ACL, enter the *acl_name* .
chassis	For the Firepower 9300 ASA security module, shows the cluster information for the chassis.
conn [**count**]	Shows the aggregated count of in-use connections for all units. If you enter the **count** keyword, only the connection count is shown.
context [*context_name*]	Shows usage per security context in multiple context mode.
cpu [**usage**]	Shows CPU usage information.
interface-mode	Shows the cluster interface mode, either spanned or individual.
memory	Shows system memory utilization and other information.
resource usage	Shows system resources and usage.
service-policy	Shows the MPF service policy statistics.
traffic	Shows traffic statistics.
xlate count	Shows current translation information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Release	Modification
9.4(1)	The **service-policy** keyword was added.
9.4(1.152)	The **chassis** keyword was added.
9.9(1)	The **context** keyword was added.

Usage Guidelines

See also the **show cluster info** and **show cluster user-identity** commands.

Examples

The following is sample output from the **show cluster access-list** command:

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www (hitcnt=0,
 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0, 0,
0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238 (hitcnt=1,
 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238 (hitcnt=0,
 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238 (hitcnt=1,
 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13 (hitcnt=0,
 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132 (hitcnt=2,
 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192 (hitcnt=3,
 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44 (hitcnt=0,
 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44 (hitcnt=429,
 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238 (hitcnt=3,
 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169 (hitcnt=2,
 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229 (hitcnt=1,
 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106 (hitcnt=0,
 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196 (hitcnt=0,
 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75 (hitcnt=0,
 0, 0, 0, 0) 0x2c7dba0d
```

To display the aggregated count of in-use connections for all units, enter:

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):***********************************************************
  100 in use, 100 most used
  cl1:******************************************************************
  100 in use, 100 most used
```

Related Commands

Command	Description
show cluster info	Shows cluster information.
show cluster user-identity	Shows cluster user identity information and statistics.

show cluster history

To view event history for the cluster, use the **show cluster history** command in privileged EXEC mode.

show cluster history [**brief**] [**latest** [*number*]] [**reverse**] [**time** [*year month day*] *hh* **:** *mm* **:** *ss*]

Syntax Description

brief	Shows cluster history without generic events.
latest [*number*]	Displays the latest events. By default, the device shows the last 512 events. You can limit the *number* of events, between 1 and 512.
reverse	Shows events in reverse order.
time [*year month day*] *hh***:***mm***:***ss*	Shows events before a specified date and time.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.14(1)	The output was enhanced to show more details for troubleshooting.
9.16(1)	We added the **brief**, **latest**, **reverse**, **time** keywords.
9.19(1)	Command output was changed from **Master** and **Slave** to **Control_Node** and **Data_Node**.

Usage Guidelines

The following is sample output from the **show cluster history time** command:

```
asa1(cfg-cluster)# show cluster history time august 26 10:10:05
==========================================================================
From State            To State              Reason
==========================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup
```

```
10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI


10:10:01 UTC Aug 26 2020
ELECTION              ONCALL                Event: Cluster unit A state is CONTROL_NODE


10:10:02 UTC Aug 26 2020
ONCALL                DATA_NODE_COLD            Data Node proceeds with configuration sync


10:10:02 UTC Aug 26 2020
DATA_NODE_COLD            DATA_NODE_CONFIG          Client progression done


10:10:04 UTC Aug 26 2020
DATA_NODE_CONFIG          DATA_NODE_FILESYS         Configuration replication finished


10:10:05 UTC Aug 26 2020
DATA_NODE_FILESYS         DATA_NODE_BULK_SYNC       Client progression done
```

The following is sample output from the **show cluster history brief** command:

```
asa1(cfg-cluster)# show cluster history brief
==========================================================================
From State            To State              Reason
==========================================================================

10:08:49 UTC Aug 26 2020
DISABLED              DISABLED              Disabled at startup


10:09:43 UTC Aug 26 2020
DISABLED              ELECTION              Enabled from CLI



10:10:02 UTC Aug 26 2020
ONCALL                DATA_NODE_COLD            Data Node proceeds with configuration sync


10:10:02 UTC Aug 26 2020
DATA_NODE_COLD            DATA_NODE_CONFIG          Client progression done


10:10:04 UTC Aug 26 2020
DATA_NODE_CONFIG          DATA_NODE_FILESYS         Configuration replication finished


10:10:05 UTC Aug 26 2020
DATA_NODE_FILESYS         DATA_NODE_BULK_SYNC       Client progression done
```

The following is sample output from the **show cluster history latest** command:

```
asa1(cfg-cluster)# show cluster history latest 3
==========================================================================
From State            To State              Reason
==========================================================================
10:10:05 UTC Aug 26 2020
DATA_NODE_FILESYS         DATA_NODE_BULK_SYNC       Client progression done


10:10:04 UTC Aug 26 2020
DATA_NODE_CONFIG          DATA_NODE_FILESYS         Configuration replication finished


10:10:02 UTC Aug 26 2020
DATA_NODE_COLD            DATA_NODE_CONFIG          Client progression done
```

Related Commands

Command	Description
show cluster	Shows aggregated data for the entire cluster and other information.
show cluster info	Shows cluster information.
show cluster user-identity	Shows cluster user identity information and statistics.

show cluster info

To view cluster information, use the **show cluster info** command in privileged EXEC mode.

show cluster info [**auto-join** | **clients** | **conn-distribution** | **counters** | **flow-mobility** | **goid** [*options*] | **health** [**details**] | **incompatible-config** | **instance-type** | **loadbalance** | **load-monitor** | **old-members** | **packet-distribution** | **trace** [*options*] | **transport** { **asp** | **cp** [**detail**] } | **unit-join-acceleration incompatible-config**]

Syntax Description

auto-join	(Optional) Shows whether the cluster node will automatically rejoin the cluster after a time delay and if the failure conditions (such as waiting for the license, chassis health check failure, and so on) are cleared. If the node is permanently disabled, or if the node is already in the cluster, then this command will not show any output.
clients	(Optional) Shows the version of register clients.
conn-distribution	(Optional) Shows the connection distribution in the cluster.
flow-mobility counters	(Optional) Shows EID movement and flow owner movement information.
goid [*options*]	(Optional) Shows the global object ID database. Options include: classmap conn-set hwidb idfw-domain idfw-group interface policymap virtual-context
health [**details**]	(Optional) Shows health monitoring information. The details keyword shows the number heartbeat message failures.
incompatible-config	(Optional) Shows commands that are incompatible with clustering in the current running configuration. This command is useful before you enable clustering.
instance-type	(Optional) Shows the ASA virtual CPU cores and RAM per cluster node.
loadbalance	(Optional) Shows load balancing information.
load-monitor	(Optional) Monitors the traffic load for cluster nodes, including total connection count, CPU and memory usage, and buffer drops. If the load is too high, you can choose to manually disable clustering on the node if the remaining nodes can handle the load, or adjust the load balancing on the external switch. This feature is enabled by default with the **load-monitor** command.

old-members	(Optional) Shows former nodes of the cluster.
packet-distribution	(Optional) Shows packet distribution in the cluster.
trace [*options*]	(Optional) Shows the clustering control module event trace. Options include: • **latest** [*number*]—Displays the latest *number* events, where the number is from 1 to 2147483647. The default is to show all. • **level** *level* —Filters events by level where the *level* is one of the following: **all** , **critical** , **debug** , **informational** , or **warning** . • **module** *module* —Filters events by module where the *module* is one of the following: **ccp** , **datapath** , **fsm** , **general** , **hc** , **license** , **rpc** , **or transport** . • **time** {[*month day*] [*hh* **:** *mm* **:** *ss*]}—Shows events before the specified time or date.
transport { **asp** | **cp** [**detail**]}	(Optional) Show transport related statistics for the following: • **asp** —Data plane transport statistics. • **cp** —Control plane transport statistics. If you enter the **detail** keyword, you can view cluster reliable transport protocol usage so you can identify packet drop issues when the buffer is full in the control plane.
unit-join-acceleration incompatible-config	(Optional) When the **unit join-acceleration** command is enabled (the default), some configuration commands are not compatible with accelerated cluster joining; if these commands are present on the node, even if accelerated cluster joining is enabled, configuration syncing will always occur. You must remove the incompatible configuration for accelerated cluster joining to work. Use the **show cluster info unit-join-acceleration incompatible-config** command to view incompatible configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.
9.3(1)	Improved support for modules in the **show cluster info health** command was added.
9.5(1)	Site ID information was added to the output.
9.5(2)	The **flow-mobility counters** keywords were added.
9.8(1)	The **health details** keyword was added.
9.9(2)	Added the **auto-join** keyword
9.9(2)	Added the **detail** keyword for **transport cp** .
9.13(1)	Added **load-monitor** and **unit-join-acceleration incompatible-config** keywords.
9.17(1)	Added the **instance-type** keyword for the ASA virtual, and added ASA virtual information to the **show cluster info** output.
9.19(1)	Command output was changed from **Master** and **Slave** to **Control_Node** and **Data_Node**.

Usage Guidelines

If you do not specify any options, the **show cluster info** command shows general cluster information including the cluster name and status, the cluster nodes, the node states, and so on.

Clear statistics using the **clear cluster info** command.

See also the **show cluster** and **show cluster user-identity** commands.

Examples

The following is sample output from the **show cluster info** command for a hardware platform:

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID : 1
      Version   : 9.5(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID : 2
      Version   : 9.5(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

The following is sample output from the **show cluster info** command for the ASA virtual:

```
Cluster ASAv-cluster: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "A" in state CONTROL_NODE
        ID        : 0
        Version   : 9.17(1)79
        Serial No.: 9A3GVQ1EL7W
        CCL IP    : 10.1.1.24
        CCL MAC   : 0050.56a8.7d4f
        Module    : ASAv
        Resource  : 2 cores / 4096 MB RAM
        Last join : 16:27:46 UTC Feb 18 2021
        Last leave: N/A
Other members in the cluster:
    Unit "B" in state DATA_NODE
        ID        : 1
        Version   : 9.17(1)79
        Serial No.: 9ACE28176EE
        CCL IP    : 10.1.1.25
        CCL MAC   : 0050.56a8.883e
        Module    : ASAv
        Resource  : 2 cores / 4096 MB RAM
        Last join : 20:29:25 UTC Feb 19 2021
        Last leave: 16:31:46 UTC Feb 19 2021
```

The following is sample output from the **show cluster info incompatible-config** command:

```
ciscoasa(cfg-cluster)# show cluster info incompatible-config
INFO: Clustering is not compatible with following commands which given a user's confirmation
 upon enabling clustering, can be removed automatically from running-config.
policy-map global_policy
 class scansafe-http
  inspect scansafe http-map fail-close
policy-map global_policy
 class scansafe-https
  inspect scansafe https-map fail-close
INFO: No manually-correctable incompatible configuration is found.
```

The following is sample output from the **show cluster info trace** command:

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

The following is sample output from the **show cluster info health** command on the ASA 5500-X:

```
ciscoasa# show cluster info health
Member ID to name mapping:
  0 - A   1 - B(myself)
                         0        1
GigabitEthernet0/0       up       up
Management0/0            up       up
ips (policy off)         up       None
sfr (policy off)         None     up
Unit overall             healthy   healthy
Cluster overall          healthy
```

The above output lists both ASA IPS (ips) and ASA FirePOWER (sfr) modules, and for each module the ASA shows “policy on” or “policy off” to show if you configured the module in the service policy. For example:

```
class-map sfr-class
match sfr-traffic
policy-map sfr-policy
class sfr-class
sfr inline fail-close
service-policy sfr interface inside
```

With the above configuration, the ASA FirePOWER module (“sfr”) will be displayed as “policy on”. If one cluster node has a module as “up”, and the other node has the module as “down” or “None”, then the node with the down module will be kicked out of the cluster. However, if the service policy is not configured, then the cluster node would not be kicked out of the cluster; the module status is only relevant if the module is running.

The following is sample output from the **show cluster info health** command on the ASA 5585-X:

```
ciscoasa# show cluster info health
spyker-13# sh clu info heal
Member ID to name mapping:
  0 - A(myself) 1 - B
                       0 1
GigabitEthernet0/0       upup
SSM Card (policy off)    upup
Unit overall             healthyhealth
Cluster overall        healthyhealth
```

If you configure the module in the service policy, then the output shows “policy on”. If you do not configure the service policy, then the output shows “policy off”, even if a module is present in the chassis.

The following is sample output from the **show cluster info flow-mobility counters** command:

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 0
EID movement notification processed : 0
Flow owner moving requested         : 0
```

The following is sample output from the **show cluster info auto-join** command:

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE
```

```
ciscoasa(cfg-cluster)# show cluster info auto-join

Unit will try to join cluster when quit reason is cleared.
Quit reason: Control Node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join

Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join

Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

See the following output for the **show cluster info transport cp detail** command:

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1
Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent
This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0
This unit as a receiver of broadcast messages
```

```
---------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256
This unit as a receiver of unicast messages
---------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303
Gated Tx Buffered Message Statistics
-------------------------------------
    current sequence number: 0
    total:                   0
    current:                 0
    high watermark:          0
    delivered:               0
    deliver failures:        0
    buffer full drops:       0
    message truncate drops:  0
    gate close ref count:    0
    num of supported clients:45
MRT Tx of broadcast messages
=============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%
Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ----------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0
MRT Tx of unitcast messages(to member_id:0)
============================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%
Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ----------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0
MRT Tx of unitcast messages(to member_id:2)
============================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%
Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
MRT Tx of unitcast messages(to member_id:3)
============================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

The following is sample output from the **show cluster info load-monitor** command:

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 25 interval:
   0           0            0            12             28
   1           0            0            13             27
```

The following is sample output from the **show cluster info unit-join-acceleration incompatible-config** command:

ciscoasa# show cluster info unit-join-acceleration incompatible-config

INFO: Clustering is not compatible with following commands. User must manually remove them to activate the cluster unit join-acceleration feature.

```
zone sf200 passive
```

The following is sample output from the show cluster info instance-type command for an ASA virtual cluster:

```
ciscoasa# show cluster info instance-type
      Unit            Module Type     CPU Cores            RAM (MB)
```

```
A                    ASAv          2                  4096
B                    ASAv          2                  4096
```

Related Commands

Command	Description
show cluster	Displays aggregated data for the entire cluster.
show cluster user-identity	Shows cluster user identity information and statistics.

show cluster user-identity

To view cluster-wide user identity information and statistics, use the **show cluster user-identity** command in privileged EXEC mode.

show cluster user-identity [**statistics** [**user** *name* | **user-group** *group_name*] | **user** [**active** [**domain** *name*] | **user** *name* | **user-group** *group_name*] [**list** [*detail*] | **all** [**list** [*detail*] | **inactive** { **domain** *name* | **user-group** *group_name*] [**list** [*detail*]] }

Syntax Description

active	Shows users with active IP-user mappings.
all	Shows all users in the user database.
domain *name*	Shows user info for a domain.
inactive	Shows users with inactive IP-user mappings.
list [*detail*]	Shows a list of users.
statistics	Shows cluster user identity statistics.
user	Shows the user database.
user *name*	Show information for a specific user.
user-group *group_name*	Shows information for each user of a specific group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

See also the **show cluster info** and **show cluster** commands.

Examples

The following is sample output from the << **command** >> command:

Related Commands

Command	Description
show cluster	Displays aggregated data for the entire cluster.
show cluster info	Shows cluster information.

show cluster vpn-sessiondb distribution

To view how active and backup sessions are distributed across the cluster, execute this command in privileged EXEC mode.

show cluster vpn-sessiondb distribution

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.9(1)	This command was added.

Usage Guidelines

This show command provides a quick view of the sessions, rather than having to execute **show vpn-sessiondb summary** on each member.

Each row contains the member id, member name, number of active sessions, and on which members the backup sessions reside.

Examples

For example, if the output of show cluster vpn-sessiondb distribution was:

Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)

Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)

Member 2 (unit-1-2): active: 0

One would read the information as:

- Member 0 has 209 active sessions, 111 sessions are backed up on member 1, 98 sessions are backed up on member 2
- Member 1 has 204 active sessions, 108 sessions are backed up on member 0, 96 sessions are backed up on member 2
- Member 2 has NO active sessions, therefore, no cluster members are backing up sessions for this node

Related Commands

Command	Description
cluster redistribute vpn-sessiondb	Redistribute the active VPN sessions on a distributed VPN cluster.

show compression

To view compression statistics on the ASA, use the **show compression** command from privileged EXEC mode.

show compression [**all | anyconnect-ssl | http-comp**]

Command Default

There is no default behavior for this command.

Syntax Description

all	Show all (anyconect-ssl, http-comp) compression statistics
anyconnect-ssl	Show AnyConnect SSL Compression statistics.
http-comp	Show HTTP-COMP Compression statistics

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following types of statistics are displayed for show compression all:

```
Compression AnyConnect Client Sessions            0
Compressed Frames                                 0
Compressed Data In (bytes)                        0
Compressed Data Out (bytes)                       0
Expanded Frames                                   0
Compression Errors                                0
Compression Resets                                0
Compression Output Buf Too Small                  0
Compression Ratio                                 0
Decompressed Frames                               0
Decompressed Data In                              0
Decompressed Data Out                             0
Decompression CRC Errors                          0
Decompression Errors                              0
Decompression Resets                              0
Decompression Ratio                               0
Block Allocation Failures                         0
```

```
Compression Skip Percent                          0%
Time Spent Compressing (peak)                   0.0%
Time Spent Decompressing (peak)                 0.0%
Number of http bytes in                          0
Number of http gzipped bytes out                 0
```

Related Commands

Command	Description
compression	Enables compression for all SVC and WebVPN connections.

show configuration

To display the configuration that is saved in flash memory on the ASA, use the **show configuration** command in privileged EXEC mode.

show configuration

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was modified.

Usage Guidelines

The show configuration command displays the saved configuration in flash memory on the ASA. Unlike the **show running-config** command, the **show configuration** command does not use many CPU resources to run.

To display the active configuration in memory (including saved configuration changes) on the ASA, use the **show running-config** command.

Examples

The following is sample output from the **show configuration** command:

```
ciscoasa# show configuration
: enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif inside
 security-level 100
 ip address 192.168.2.5 255.255.255.0
!
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.132.12.6 255.255.255.0
!
interface Ethernet0/2
```

```
 nameif dmz
 security-level 50
 ip address 10.0.0.5 255.255.0.0
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 192.168.1.1 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/newImage
ftp mode passive
access-list acl1 extended permit ip any any
access-list mgcpacl extended permit udp any any eq 2727
access-list mgcpacl extended permit udp any any eq 2427
access-list mgcpacl extended permit udp any any eq tftp
access-list mgcpacl extended permit udp any any eq 1719
access-list permitIp extended permit ip any any
pager lines 25
logging enable
logging console debugging
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
mtu management 1500
icmp unreachable rate-limit 1 burst-size 1
icmp permit any inside
icmp permit any outside
icmp permit any dmz
asdm image disk0:/pdm
no asdm history enable
arp timeout 14400
global (outside) 1 10.132.12.50-10.132.12.52
global (outside) 1 interface
global (dmz) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
access-group permitIp in interface inside
access-group permitIp in interface outside
access-group mgcpacl in interface dmz
!
router ospf 1
 network 10.0.0.0 255.255.0.0 area 192.168.2.0
 network 192.168.2.0 255.255.255.0 area 192.168.2.0
 log-adj-changes
 redistribute static subnets
 default-information originate
!
route outside 0.0.0.0 0.0.0.0 10.132.12.1 1
route outside 10.129.0.0 255.255.0.0 10.132.12.1 1
route outside 88.0.0.0 255.0.0.0 10.132.12.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
```

```
dynamic-access-policy-record DfltAccessPolicy
aaa authentication ssh console LOCAL
http server enable
http 10.132.12.0 255.255.255.0 outside
http 192.168.2.0 255.255.255.0 inside
http 192.168.1.0 255.255.255.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet 192.168.2.0 255.255.255.0 inside
telnet 10.132.12.0 255.255.255.0 outside
telnet timeout 5
ssh 192.168.2.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
!
threat-detection basic-threat
threat-detection statistics access-list
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect mgcp
policy-map type inspect mgcp mgcpapp
 parameters
  call-agent 150.0.0.210 101
  gateway 50.0.0.201 101
  gateway 100.0.0.201 101
  command-queue 150
!
service-policy global_policy global
webvpn
 memory-size percent 25
 enable inside
 internal-password enable
 onscreen-keyboard logon
username snoopy password /JcYsjvxHfBHc4ZK encrypted
prompt hostname context
Cryptochecksum:62bf8f5de9466cdb64fe758079594635:
end
```

Related Commands

Command	Description
configure	Configures the ASA from the terminal.

show configuration session

To display the current configuration sessions and the changes within the sessions, use the **show configuration session** command in privileged EXEC mode.

show configuration session [*session_name*]

Syntax Description

session_name	The name of an existing configuration session. If you omit this parameter, all existing sessions are shown.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Use this command in conjunction with the **configure session** command, which creates isolated sessions for editing ACLs and their objects. This command shows the names of the sessions, and all of the configuration changes that have been made in the sessions.

If a session shows as committed, you can open the session and revert the changes if you decide they did not work as expected.

Examples

The following example shows all available sessions:

```
ciscoasa# show configuration session

config-session abc (un-committed)
 access-list abc permit ip any any
 access-list abc permit tcp any any

config-session abc2 (un-committed)
 object network test
 host 1.1.1.1
 object network test2
 host 2.2.2.2

ciscoasa#
```

Related Commands

Command	Description
clear configuration session	Deletes a configuration session and its contents.
clear session	Clears the contents of a configuration session or resets its access flag.
configure session	Creates or opens a session.

show conn

To display the connection state for the designated connection type, use the show **conn** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show conn [**count** | [**all**] [**detail** [**data-rate-filter** { **lt | eq | gt** } *value*]] [**long**] [**state** *state_type*] [**protocol** { **tcp | udp | sctp** }] [**scansafe**] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*]] [**port** *src_port* [*-src_port*]] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*]] [**port** *dest_port* [*-dest_port*]] [**user-identity | user** [*domain_nickname* \ ] *user_name* **| user-group** [*domain_nickname* \\ ] *user_group_name*] | **security-group**] [**zone** *zone_name* [**zone** *zone_name*] [**...**]] [**data-rate**]

Syntax Description

address	(Optional) Displays connections with the specified source or destination IP address.
all	(Optional) Displays connections that are to the device or from the device, in addition to through-traffic connections.
count	(Optional) Displays the number of active connections.
dest_ip	(Optional) Specifies the destination IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
dest_port	(Optional) Specifies the destination port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
detail	(Optional) Displays connections in detail, including translation type and interface information.
data-rate-filter { **lt | eq | gt** } *value*	(Optional) Displays connections that are filtered based on a data-rate value (bytes per second). For example: `data-rate-filter gt 123`
long	(Optional) Displays connections in long format.
netmask *mask*	(Optional) Specifies a subnet mask for use with the given IP address.
port	(Optional) Displays connections with the specified source or destination port.
protocol { **tcp | udp | sctp** }	(Optional) Specifies the connection protocol.
scansafe	(Optional) Shows connections being forwarded to the Cloud Web Security server.
security-group	(Optional) Specifies that all connections displayed belong to the specified security group.

src_ip	(Optional) Specifies the source IP address (IPv4 or IPv6). To specify a range, separate the IP addresses with a dash (-). For example: `10.1.1.1-10.1.1.5`
src_port	(Optional) Specifies the source port number. To specify a range, separate the port numbers with a dash (-). For example: `1000-2000`
state *state_type*	(Optional) Specifies the connection state type. See <xref> for a list of the keywords available for connection state types.
user [*domain_nickname* \ ] *user_name*	(Optional) Specifies that all connections displayed belong to the specified user. When you do not include the *domain_nickname* argument, the ASA displays information for the user in the default domain.
user-group [*domain_nickname* \\ ] *user_group_name*	(Optional) Specifies that all connections displayed belong to the specified user group. When you do not include the *domain_nickname* argument, the ASA displays information for the user group in the default domain.
user-identity	(Optional) Specifies that the ASA display all connections for the Identity Firewall feature. When displaying the connections, the ASA displays the user name and IP address when it identifies a matching user. Similarly, the ASA displays the host name and an IP address when it identifies a matching host.
zone [*zone_name*]	(Optional) Displays connections for a zone. The **long** and **detail** keywords show the primary interface on which the connection was built and the current interface used to forward the traffic.
data-rate	(Optional) Displays whether data-rate tracking status is enabled or disabled.

Command Default

All through connections are shown by default. You need to use the **all** keyword to also view management connections to the device.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(8)/7.2(4)/8.0(4)	The syntax was simplified to use source and destination concepts instead of "local" and "foreign." In the new syntax, the source address is the first address entered and the destination is the second address. The old syntax used keywords like **foreign** and **fport** to determine the destination address and port.
7.2(5)/8.0(5)/8.1(2)/8.2(4)/8.3(2)	The **tcp_embryonic** state type was added. This type shows all TCP connections with the i flag (incomplete connections); i flag connections for UDP are not shown.
8.2(1)	The b flag was added for TCP state bypass.
8.4(2)	The **user-identity** , **user** , and **user-group** keywords were added to support the Identity Firewall.
9.0(1)	Support for clustering was added. We added the **scansafe** and **security-group** keywords.
9.3(2)	The **zone** keyword was added.
9.5(2)	The L flag was added for traffic subject to LISP flow-mobility.
9.5(2)	The Q flag for detailed output was added for Diameter connections. The **protocol sctp** keyword was added. The o flag for detailed output was added for off-loaded flows.
9.6(2)	The u flag for detailed output was added for STUN connections. The v flag was added for M3UA connections.
9.7(1)	The l flag was added to indicate the stub flow is local director Yl or local backup yl when using cluster director localization.
9.9(1)	VPN Stub at the end of the detail output, indicating that the connection is playing the role of a VPN encryption stub flow in addition to its cluster role.
9.13(1)	Dead Connection Detection (DCD) initiator/responder probe counts were added to the **show conn detail** output for DCD-enabled connections.
9.14(1)	Connection data-rate tracking status was added. The **data-rate-filter** keyword was added to the **show conn detail** command to filter the connections by user-specified data rate value.
9.16(1)	Multicast data connection entries were no longer displayed in the output. The entries were moved to the **show local-host** output.

Usage Guidelines

The show conn command displays the number of active TCP and UDP connections, and provides information about connections of various types. Use the **show conn all** command to see the entire table of connections.

Note When the ASA creates a pinhole to allow secondary connections, this is shown as an incomplete conn by the **show conn** command. To clear this incomplete conn use the **clear conn** command.

The connection types that you can specify using the **show conn state** command are defined in Table 38: Connection State Types. When specifying multiple connection types, use commas without spaces to separate the keywords.

Table 38: Connection State Types

Keyword	Connection Type Displayed
up	Connections in the up state.
conn_inbound	Inbound connections.
ctiqbe	CTIQBE connections
data_in	Inbound data connections.
data_out	Outbound data connections.
finin	FIN inbound connections.
finout	FIN outbound connections.
h225	H.225 connections
h323	H.323 connections
http_get	HTTP get connections.
mgcp	MGCP connections.
nojava	Connections that deny access to Java applets.
rpc	RPC connections.
service_module	Connections being scanned by an SSM.
sip	SIP connections.
skinny	SCCP connections.
smtp_data	SMTP mail data connections.
sqlnet_fixup_data	SQL*Net data inspection engine connections.
tcp_embryonic	TCP embryonic connections.
vpn_orphan	Orphaned VPN tunneled flows.

Usage Guidelines

When you use the detail option, the system displays information about the translation type and interface information using the connection flags defined in Table 38: Connection State Types. Also, VPN stub may be shown at the end of the output of this command indicating that the connection is playing the role of a VPN encryption stub flow in addition to its cluster role. A VPN stub is used to encrypt clear text packets in an asymmetric VPN traffic scenario or hub-n-spoke scenario.

Table 39: Connection Flags

Flag	Description
a	awaiting outside ACK to SYN
A	awaiting inside ACK to SYN
b	TCP state bypass
B	initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE) media connection
d	dump
D	DNS
E	outside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PASV command and the outside server accepts, the ASA preallocates an outside back connection with this flag set. If the inside client attempts to connect back to the server, then the ASA denies this connection attempt. Only the outside server can use the preallocated secondary connection.
f	inside FIN
F	outside FIN
g	Media Gateway Control Protocol (MGCP) connection
G	connection is part of a group[1]
h	H.225
H	H.323
i	incomplete TCP or UDP connection
I	inbound data
k	Skinny Client Control Protocol (SCCP) media connection
K	GTP t3-response
l	local director/backup stub flow
L	traffic subject to LISP flow-mobility
m	SIP media connection

Flag	Description
M	SMTP data
o	Off-loaded flow.
O	outbound data
p	replicated (unused)
P	inside back connection. This is a secondary data connection that must be initiated from the inside host. For example, using FTP, after the inside client issues the PORT command and the outside server accepts, the ASA preallocates an inside back connection with this flag set. If the outside server attempts to connect back to the client, then the ASA denies this connection attempt. Only the inside client can use the preallocated secondary connection.
q	SQL*Net data
Q	Diameter connection
r	inside acknowledged FIN
R	outside acknowledged FIN for TCP connection
R	UDP RPC[2]
s	awaiting outside SYN
S	awaiting inside SYN
t	SIP transient connection[3]
T	SIP connection[4]
u	STUN connection
U	up
v	M3UA connection
V	VPN orphan
w	For inter-chassis clustering on the Firepower 9300, identifies a flow on a backup owner on a separate chassis.
W	WAAS
X	Inspected by the service module, such as a CSC SSM.
y	For clustering, identifies a backup owner flow.
Y	For clustering, identifies a director flow.
z	For clustering, identifies a forwarder flow.

Flag	Description
Z	Cloud Web Security

[1] The G flag indicates the connection is part of a group. It is set by the GRE and FTP Strict inspections to designate the control connection and all its associated secondary connections. If the control connection terminates, then all associated secondary connections are also terminated.
[2] Because each row of show conn command output represents one connection (TCP or UDP), there will be only one R flag per row.
[3] For UDP connections, the value t indicates that it will timeout after one minute.
[4] For UDP connections, the value T indicates that the connection will timeout according to the value specified using the timeout sip command.

Note For connections using a DNS server, the source port of the connection may be replaced by the *IP address of DNS server* in the **show conn** command output.

A single connection is created for multiple DNS sessions, as long as they are between the same two hosts, and the sessions have the same 5-tuple (source/destination IP address, source/destination port, and protocol). DNS identification is tracked by app_id, and the idle timer for each app_id runs independently.

Because the app_id expires independently, a legitimate DNS response can only pass through the ASA within a limited period of time and there is no resource build-up. However, when you enter the **show conn** command, you will see the idle timer of a DNS connection being reset by a new DNS session. This is due to the nature of the shared DNS connection and is by design.

Note When there is no TCP traffic for the period of inactivity defined by the **timeout conn** command (by default, 1:00:00), the connection is closed and the corresponding conn flag entries are no longer displayed.

If a LAN-to-LAN/Network-Extension Mode tunnel drops and does not come back, there might be a number of orphaned tunnel flows. These flows are not torn down as a result of the tunnel going down, but all the data attempting to flow through them is dropped. The **show conn** command output shows these orphaned flows with the **V** flag.

When the following TCP connection directionality flags are applied to connections between same-security interfaces (see the **same-security permit** command), the direction in the flag is not relevant because for same-security interfaces, there is no “inside” or “outside.” Because the ASA has to use these flags for same-security connections, the ASA may choose one flag over another (for example, f vs. F) based on other connection characteristics, but you should ignore the directionality chosen.

- B—Initial SYN from outside
- a—Awaiting outside ACK to SYN
- A—Awaiting inside ACK to SYN
- f—Inside FIN
- F—Outside FIN
- s—Awaiting outside SYN

- S—Awaiting inside SYN

To display information for a specific connection, include the **security-group** keyword and specify a security group table value or security group name for both the source and destination of the connection. The ASA displays the connection matching the specific security group table values or security group names.

When you specify the **security-group** keyword without specifying a source and destination security group table value or a source and destination security group name, the ASA displays data for all SXP connections.

The ASA displays the connection data in the format *security_group_name* (*SGT_value*) or just as the *SGT_value* when the security group name is unknown.

Note Security group data is not available for stub connections because stub connection do not go through the slow path. Stub connections maintain only the information necessary to forward packets to the owner of the connection.

You can specify a single security group name to display all connections in a cluster; for example, the following example displays connections matching security-group mktg in all units of the cluster:

```
ciscoasa# show cluster conn security-group name mktg
```

Use the **data-rate** keyword to view the current state of the connection data rate tracking feature—enabled or disabled. Use the **data-rate filte** r keyword to filter the connections based on the data-rate value in bytes per second. Use the relational operators (lesser than, equal to, or greater than) to filter the connections data. The output displays the active connections along with two data rate values—instantaneous one-second and maximum data rate, for both forward and reverse flows.

Examples

When specifying multiple connection types, use commas without spaces to separate the keywords. The following example displays information about RPC, H.323, and SIP connections in the Up state:

```
ciscoasa# show conn state up,rpc,h323,sip
```

The following is sample output from the **show conn count** command:

```
ciscoasa# show conn count
54 in use, 123 most used
```

The following is sample output from the**show conn** command. This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 10.10.49.10. Because there is no B flag, the connection is initiated from the inside. The “U”, “I”, and “O” flags denote that the connection is active and has received inbound and outbound data.

```
ciscoasa# show conn
54 in use, 123 most used
TCP out 10.10.49.10:23 in 10.1.1.15:1026 idle 0:00:22, bytes 1774, flags UIO
UDP out 10.10.49.10:31649 in 10.1.1.15:1028 idle 0:00:14, bytes 0, flags D-
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:5060, idle 0:00:24, bytes 1940435, flags UTIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:5060, idle 0:00:42, bytes 2328346, flags UTIOB
TCP dmz 10.10.10.51:50196 inside 192.168.1.22:2000, idle 0:00:04, bytes 31464, flags UIB
TCP dmz 10.10.10.51:52738 inside 192.168.1.21:2000, idle 0:00:09, bytes 129156, flags UIOB
TCP dmz 10.10.10.50:49764 inside 192.168.1.21:0, idle 0:00:42, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):49736 inside 192.168.1.21:0, idle 0:01:32, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:00:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:01:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:02:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:03:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:04:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:05:34, bytes 0,
flags Ti
TCP dmz 10.10.10.50:50026 inside 192.168.1.22:0, idle 0:06:24, bytes 0, flags Ti
TCP outside 192.168.1.10(20.20.20.24):50663 inside 192.168.1.22:0, idle 0:07:34, bytes 0,
flags Ti
```

The following is sample output from the **show conn**command, whcih includes the “X” flag to indicate that the connection is being scanned by the SSM.

```
ciscoasa# show conn address 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03, bytes 2733, flags UIOX
```

The following is sample output from the **show conn detail**command. This example shows a UDP connection from outside host 10.10.49.10 to inside host 10.1.1.15. The D flag denotes that this is a DNS connection. The number 1028 is the DNS ID over the connection.

```
ciscoasa# show conn detail
54 in use, 123 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       l - local director/backup stub flow
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, u - STUN,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
Cluster units to ID mappings:
  ID 0: asa1
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
TCP outside:10.10.49.10/23 inside:10.1.1.15/1026,
    flags UIO, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
UDP outside:10.10.49.10/31649 inside:10.1.1.15/1028,
    flags dD, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/50026 inside:192.168.1.22/5060,
    flags UTIOB, idle 39s, uptime 1D19h, timeout 1h0m, bytes 1940435
TCP dmz:10.10.10.50/49764 inside:192.168.1.21/5060,
    flags UTIOB, idle 56s, uptime 1D19h, timeout 1h0m, bytes 2328346
TCP dmz:10.10.10.51/50196 inside:192.168.1.22/2000,
    flags UIB, idle 18s, uptime 1D19h, timeout 1h0m, bytes 31464
TCP dmz:10.10.10.51/52738 inside:192.168.1.21/2000,
    flags UIOB, idle 23s, uptime 1D19h, timeout 1h0m, bytes 129156
TCP outside:10.132.64.166/52510 inside:192.168.1.35/2000,
    flags UIOB, idle 3s, uptime 1D21h, timeout 1h0m, bytes 357405
TCP outside:10.132.64.81/5321 inside:192.168.1.22/5060,
    flags UTIOB, idle 1m48s, uptime 1D21h, timeout 1h0m, bytes 2083129
TCP outside:10.132.64.81/5320 inside:192.168.1.21/5060,
    flags UTIOB, idle 1m46s, uptime 1D21h, timeout 1h0m, bytes 2500529
TCP outside:10.132.64.81/5319 inside:192.168.1.22/2000,
    flags UIOB, idle 31s, uptime 1D21h, timeout 1h0m, bytes 32718
TCP outside:10.132.64.81/5315 inside:192.168.1.21/2000,
    flags UIOB, idle 14s, uptime 1D21h, timeout 1h0m, bytes 358694
TCP outside:10.132.64.80/52596 inside:192.168.1.22/2000,
    flags UIOB, idle 8s, uptime 1D21h, timeout 1h0m, bytes 32742
TCP outside:10.132.64.80/52834 inside:192.168.1.21/2000,
    flags UIOB, idle 6s, uptime 1D21h, timeout 1h0m, bytes 358582
TCP outside:10.132.64.167/50250 inside:192.168.1.35/2000,
    flags UIOB, idle 26s, uptime 1D21h, timeout 1h0m, bytes 375617
```

The following is sample output from the **show conn** command when an orphan flow exists, as indicated by the **V** flag:

```
ciscoasa# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle 0:00:00, bytes 1048, flags UIOB
```

To limit the report to those connections that have orphan flows, add the **vpn_orphan** option to the **show conn state** command, as in the following example:

```
ciscoasa# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013, idle 0:00:00, bytes 2841019, flags
UOVB
```

For clustering, to troubleshoot the connection flow, first see connections on all units by entering the **cluster exec show conn** command on the master unit. Look for flows that have the following flags: director (Y), backup (y), and forwarder (z). The following example shows an SSH connection from 172.18.124.187:22 to 192.168.103.131:44727 on all three ASAs; ASA 1 has the z flag showing it is a forwarder for the connection, ASA3 has the Y flag showing it is the director for the connection, and ASA2 has no special flags showing it is the owner. In the outbound direction, the packets for this connection enter the inside interface on ASA2 and exit the outside interface. In the inbound direction, the packets for this connection enter the outside interface on ASA 1 and ASA3, are forwarded over the cluster control link to ASA2, and then exit the inside interface on ASA2.

```
ciscoasa/ASA1/master# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes 37240828,
 flags z
ASA2:*****************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes 37240828,
 flags UIO
ASA3:*****************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
```

```
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes 0, flags
  Y
```

The output of **show conn detail** on ASA2 shows that the most recent forwarder was ASA1:

```
ciscoasa/ASA2/slave# show conn detail
12 in use, 13 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 1 in use, 61 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       l - local director/backup stub flow
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, u - STUN,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
Cluster units to ID mappings:
  ID 0: asa1
  ID 1: asa2
  ID 255: The default cluster member ID which indicates no ownership or affiliation
          with an existing cluster member
TCP outside: 172.18.124.187/22 inside: 192.168.103.131/44727,
    flags UIO , idle 0s, uptime 25s, timeout 1h0m, bytes 1036044, cluster sent/rcvd bytes
0/1032983, cluster sent/rcvd total bytes 0/1080779, owners (1,255)
Traffic received at interface outside
        Locally received: 0 (0 byte/s)
        From most recent forwarder ASA1: 1032983 (41319 byte/s)
Traffic received at interface inside
        Locally received: 3061 (122 byte/s)
```

The following examples show how to display connections for the Identity Firewall feature:

```
ciscoasa# show conn user-identity
1219 in use, 1904 most used
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00, bytes
 10, flags -
UDP inside (www.yahoo.com)10.0.0.2:1586 outside (user2)192.0.0.1:30000, idle 0:00:00, bytes
 10, flags –
UDP inside 10.0.0.34:1586 outside 192.0.0.25:30000, idle 0:00:00, bytes 10, flags –
...
ciscoasa# show conn user user1
2 in use
UDP inside (www.yahoo.com))10.0.0.2:1587 outside (user1)192.0.0.2:30000, idle 0:00:00, bytes
 10, flags –
```

See the following output for the **show conn long zone** command:

```
ciscoasa# show conn long zone zone-inside zone zone-outside
TCP outside-zone:outside1(outside2): 10.122.122.1:1080 inside-zone:inside1(inside2):
10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

When you use the **detail** keyword, you can see information about Dead Connection Detection (DCD) probing, which shows how often the connection was probed by the initiator and responder. For example, the connection details for a DCD-enabled connection would look like the following:

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828, cluster sent/rcvd bytes
0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

The following example shows how to view the status of connection data-rate tracking feature:

```
ciscoasa# show conn data-rate
Connection data rate tracking is currently enabled.
```

The following example shows how to filter the connection based on a specified data-rate:

```
ciscoasa# show conn detail data-rate-filter ?
eq  Enter this keyword to show conns with data-rate equal to specified value
gt   Enter this keyword to show conns with data-rate greater than specified
       value
lt    Enter this keyword to show conns with data-rate less than specified value
ciscoasa# show conn detail data-rate-filter gt ?
<0-4294967295>  Specify the data rate value in bytes per second
ciscoasa# show conn detail data-rate-filter gt 123 | grep max rate
    max rate:     3223223/399628 bytes/sec
    max rate:     3500123/403260 bytes/sec
```

Related Commands

Commands	Description
clear conn	Clears connections.
clear conn data-rate	Clears the current maximum data-rate stored.

show console-output

To display the currently captured console output, use the **show console-output** command in privileged EXEC mode.

show console-output

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show console-output** command, which displays the following message when there is no console output:

```
ciscoasa# show console-output
Sorry, there are no messages to display
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
clear configure timeout	Restores the default idle time durations in the configuration.
console timeout	Sets the idle timeout for a console connection to the ASA.
show running-config console timeout	Displays the idle timeout for a console connection to the ASA.

show context

To show context information including allocated interfaces and the configuration file URL, the number of contexts configured, or from the system execution space, a list of all contexts, use the **show context** command in privileged EXEC mode.

show context [*name* | **detail** | **count**]

Syntax Description

count	(Optional) Shows the number of contexts configured.
detail	(Optional) Shows additional detail about the context(s) including the running state and information for internal use.
name	(Optional) Sets the context name. If you do not specify a name, the ASA displays all contexts. Within a context, you can only enter the current context name.

Command Default

In the system execution space, the ASA displays all contexts if you do not specify a name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	Information about assigned IPS virtual sensors was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show context** command. The following sample display shows three contexts:

```
ciscoasa# show context
Context Name      Interfaces                    URL
*admin            GigabitEthernet0/1.100        flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200        flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300        flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

Table 40: show context Fields shows each field description.

Table 40: show context Fields

Field	Description
Context Name	Lists all context names. The context name with the asterisk (*) is the admin context.
Interfaces	The interfaces assigned to the context.
URL	The URL from which the ASA loads the context configuration.

Examples

The following is sample output from the **show context detail** command in the system execution space:

```
ciscoasa# show context detail
Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Real IPS Sensors: ips1, ips2
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000013, ID: 1
Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Real IPS Sensors: ips1, ips3
  Mapped IPS Sensors: highsec, lowsec
  Flags: 0x00000011, ID: 2
Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257
Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

Table 41: Context States shows each field description.

Table 41: Context States

Field	Description
Context	The context name. The null context information is for internal use only. The system context represents the system execution space.
State Message:	The context state. See the possible messages below.

Field	Description
Has been created, but initial ACL rules not complete	The ASA parsed the configuration but has not yet downloaded the default ACLs to establish the default security policy. The default security policy applies to all contexts initially, and includes disallowing traffic from lower security levels to higher security levels, enabling application inspection, and other parameters. This security policy ensures that no traffic can pass through the ASA after the configuration is parsed but before the configuration ACLs are compiled. You are unlikely to see this state because the configuration ACLs are compiled very quickly.
Has been created, but not initialized	You entered the **context** *name* command, but have not yet entered the **config-url** command.
Has been created, but the config hasn't been parsed	The default ACLs were downloaded, but the ASA has not parsed the configuration. This state might exist because the configuration download might have failed because of network connectivity issues, or you have not yet entered the **config-url** command. To reload the configuration, from within the context, enter **copy startup-config running-config** . From the system, reenter the **config-url** command. Alternatively, you can start configuring the blank running configuration.
Is a system resource	This state applies only to the system execution space and to the null context. The null context is used by the system, and the information is for internal use only.
Is a zombie	You deleted the context using the **no context** or **clear context** command, but the context information persists in memory until the ASA reuses the context ID for a new context, or you restart.
Is active	This context is currently running and can pass traffic according to the context configuration security policy.
Is ADMIN and active	This context is the admin context and is currently running.
Was a former ADMIN, but is now a zombie	You deleted the admin context using the **clear configure context** command, but the context information persists in memory until the ASA reuses the context ID for a new context, or you restart.
Real Interfaces	The interfaces assigned to the context. If you mapped the interface IDs in the **allocate-interface** command, this display shows the real name of the interface.
Mapped Interfaces	If you mapped the interface IDs in the **allocate-interface** command, this display shows the mapped names. If you did not map the interfaces, the display lists the real names again.
Real IPS Sensors	The IPS virtual sensors assigned to the context if you have an AIP SSM installed. If you mapped the sensor names in the **allocate-ips** command, this display shows the real name of the sensor.
Mapped IPS Sensors	If you mapped the sensor names in the **allocate-ips** command, this display shows the mapped names. If you did not map the sensor names, the display lists the real names again.

Field	Description
Flag	For internal use only.
ID	An internal ID for this context.

Examples

The following is sample output from the **show context count** command:

```
ciscoasa# show context count
Total active contexts: 2
```

Related Commands

Command	Description
admin-context	Sets the admin context.
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts or the system execution space.
config-url	Specifies the location of the context configuration.
context	Creates a security context in the system configuration and enters context configuration mode.

show controller

To view controller-specific information of all interfaces present, use the **show controller** command in privileged EXEC mode.

show controller [**slot**] [*physical_interface*] [**pci** [**bridge** [*bridge-id* [*port-num*]]]] [**detail**]

Syntax Description

bridge	(Optional) Displays PCI bridge-specific information for the ASA 5585-X.
bridge-id	(Optional) Displays each unique PCI bridge identifier for the ASA 5585-X.
detail	(Optional) Shows additional detail about the controller.
pci	(Optional) Displays a summary of PCI devices along with their first 256 bytes of PCI configuration space for the ASA 5585-X.
physical_interface	(Optional) Identifies the interface ID.
port-num	(Optional) Displays the unique port number within each PCI bridge for the ASA 5585-X adaptive ASA.
slot	(Optional) Displays PCI-e bus and slot information for the ASA 5580 only.

Command Default

If you do not identify an interface, this command shows information for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	This command now applies to all platforms, and not just the ASA 5505. The **detail** keyword was added.
8.1(1)	The **slot** keyword was added for the ASA 5580.
8.2(5)	The **pci** , **bridge** , *bridge-id,* and *port-num* options were added for the ASA 5585-X with an IPS SSP installed. In addition, support for sending pause frames to enable flow control on 1 GigabitEthernet interfaces has been added for all ASA models.

Release	Modification
8.6(1)	Support was added for the **detail** keyword for the ASA 5512-X through ASA 5555-X Internal-Control0/0 interface, used for control traffic between the ASA and the software module, and for the Internal-Data0/1 interface used for data traffic to the ASA and the software module.

Usage Guidelines

This command helps Cisco TAC gather useful debug information about the controller when investigating internal and customer found defects. The actual output depends on the model and Ethernet controller. The command also displays information about all the PCI bridges of interest in the ASA 5585-X with an IPS SSP installed. For the ASA Services Module, the **show controller** command output does not show any PCIe slot information.

Examples

The following is sample output from the **show controller** command:

```
ciscoasa# show controller
Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
     Global Registers:
         Control:       0x0482
---------------------------------------------------------------------
Number of VLANs: 1
---------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
---------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
---------------------------------------------------------------------
....
Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
```

```
            Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
            VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
            Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
            Port Asc Vt:   0x0002
            In Discard Lo: 0x0000  In Discard Hi: 0x0000
            In Filtered:   0x0000  Out Filtered:  0x0000
      ----Inline power related counters and registers----
      Power on fault: 0  Power off fault: 0
      Detect enable fault: 0  Detect disable fault: 0
      Faults: 0
      Driver counters:
      I2C Read Fail: 0   I2C Write Fail: 0
      Resets: 1  Initialized: 1
      PHY reset error: 0
      LTC4259 registers:
      INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
      DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
      SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
      PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
      OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
      TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00
...
Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                           0xe0004000 = 0x00000000
    ctrl_status                   0xe0004004 = 0x5501064a
    irq_src                       0xe0004008 = 0x00000000
    irq_msk                       0xe000400c = 0x00000000
    irq_hw_err_src                0xe0004010 = 0x00000000
    irq_hw_err_msk                0xe0004014 = 0x00001000
    bmu_cs_rxq                    0xe0004060 = 0x002aaa80
    bmu_cs_stxq                   0xe0004068 = 0x01155540
    bmu_cs_atxq                   0xe000406c = 0x012aaa80
   Bank 2: MAC address registers:

....
```

The following is sample output from the **show controller detail** command:

```
ciscoasa# show controller gigabitethernet0/0 detail
GigabitEthernet0/0:
   Intel i82546GB revision 03
     Main Registers:
         Device Control:              0xf8260000 = 0x003c0249
         Device Status:               0xf8260008 = 0x00003347
         Extended Control:            0xf8260018 = 0x000000c0
         RX Config:                   0xf8260180 = 0x0c000000
         TX Config:                   0xf8260178 = 0x000001a0
         RX Control:                  0xf8260100 = 0x04408002
         TX Control:                  0xf8260400 = 0x000400fa
         TX Inter Packet Gap:         0xf8260410 = 0x00602008
         RX Filter Cntlr:             0xf8260150 = 0x00000000
         RX Chksum:                   0xf8265000 = 0x00000300
     RX Descriptor Registers:
         RX Descriptor 0 Cntlr:       0xf8262828 = 0x00010000
         RX Descriptor 0 AddrLo:      0xf8262800 = 0x01985000
         RX Desccriptor 0 AddrHi:     0xf8262804 = 0x00000000
         RX Descriptor 0 Length:      0xf8262808 = 0x00001000
         RX Descriptor 0 Head:        0xf8262810 = 0x00000000
         RX Descriptor 0 Tail:        0xf8262818 = 0x000000ff
         RX Descriptor 1 Cntlr:       0xf8262828 = 0x00010000
         RX Descriptor 1 AddrLo:      0xf8260138 = 0x00000000
         RX Descriptor 1 AddrHi:      0xf826013c = 0x00000000
         RX Descriptor 1 Length:      0xf8260140 = 0x00000000
```

```
        RX Descriptor 1 Head:       0xf8260148 = 0x00000000
        RX Descriptor 1 Tail:       0xf8260150 = 0x00000000
    TX Descriptor Registers:
        TX Descriptor 0 Cntlr:      0xf8263828 = 0x00000000
        TX Descriptor 0 AddrLo:     0xf8263800 = 0x01987000
        TX Descriptor 0 AddrHi:     0xf8263804 = 0x00000000
        TX Descriptor 0 Length:     0xf8263808 = 0x00001000
        TX Descriptor 0 Head:       0xf8263810 = 0x00000000
        TX Descriptor 0 Tail:       0xf8263818 = 0x00000000
    RX Address Array:
        Ethernet Address 0:         0012.d948.ef58
        Ethernet Address 1:         Not Valid!
        Ethernet Address 2:         Not Valid!
        Ethernet Address 3:         Not Valid!
        Ethernet Address 4:         Not Valid!
        Ethernet Address 5:         Not Valid!
        Ethernet Address 6:         Not Valid!
        Ethernet Address 7:         Not Valid!
        Ethernet Address 8:         Not Valid!
        Ethernet Address 9:         Not Valid!
        Ethernet Address a:         Not Valid!
        Ethernet Address b:         Not Valid!
        Ethernet Address c:         Not Valid!
        Ethernet Address d:         Not Valid!
        Ethernet Address e:         Not Valid!
        Ethernet Address f:         Not Valid!
    PHY Registers:
        Phy Control:                0x1140
        Phy Status:                 0x7969
        Phy ID 1:                   0x0141
        Phy ID 2:                   0x0c25
        Phy Autoneg Advertise:      0x01e1
        Phy Link Partner Ability:   0x41e1
        Phy Autoneg Expansion:      0x0007
        Phy Next Page TX:           0x2801
        Phy Link Partnr Next Page:  0x0000
        Phy 1000T Control:          0x0200
        Phy 1000T Status:           0x4000
        Phy Extended Status:        0x3000
    Detailed Output - RX Descriptor Ring:
    rx_bd[000]: baddr      = 0x019823A2, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000
    rx_bd[001]: baddr      = 0x01981A62, length = 0x0000, status  = 0x00
                pkt chksum = 0x0000,     errors = 0x00,   special = 0x0000

 .......
```

The following is sample output from the **show controller detail** command for the Internal interfaces on the ASA 5512-X through ASA 5555-X:

```
ciscoasa# show controller detail
Internal-Control0/0:
   ASA IPS/VM Back Plane TunTap Interface , port id 9
     Major Configuration Parameters
         Device Name           : en_vtun
         Linux Tun/Tap Device  : /dev/net/tun/tap1
         Num of Transmit Rings : 1
         Num of Receive Rings  : 1
         Ring Size             : 128
         Max Frame Length      : 1550
         Out of Buffer         : 0
         Reset                 : 0
         Drop                  : 0
```

```
      Transmit Ring [0]:
          tx_pkts_in_queue      : 0
          tx_pkts               : 176
          tx_bytes              : 9664
      Receive Ring [0]:
          rx_pkts_in_queue      : 0
          rx_pkts               : 0
          rx_bytes              : 0
          rx_drops              : 0
Internal-Data0/1:
   ASA IPS/VM Management Channel TunTap Interface , port id 9
      Major Configuration Parameters
          Device Name           : en_vtun
          Linux Tun/Tap Device  : /dev/net/tun/tap2
          Num of Transmit Rings : 1
          Num of Receive Rings  : 1
          Ring Size             : 128
          Max Frame Length      : 1550
          Out of Buffer         : 0
          Reset                 : 0
          Drop                  : 0
      Transmit Ring [0]:
          tx_pkts_in_queue      : 0
          tx_pkts               : 176
          tx_bytes              : 9664
      Receive Ring [0]:
          rx_pkts_in_queue      : 0
          rx_pkts               : 0
          rx_bytes              : 0
          rx_drops              : 0
```

The following is sample output from the **show controller slot** command:

```
Slot  Card Description                               PCI-e Bandwidth Cap.
----  ----------------                               ----------------------
3.    ASA 5580 2 port 10GE SR Fiber Interface Card   Bus: x4, Card: x8
4.    ASA 5580 4 port GE Copper Interface Card       Bus: x4, Card: x4
5.    ASA 5580 2 port 10GE SR Fiber Interface Card   Bus: x8, Card: x8
6.    ASA 5580 4 port GE Fiber Interface Card        Bus: x4, Card: x4
7.    empty                                          Bus: x8
8.    empty                                          Bus: x8
```

The following is sample output from the **show controller pci** command:

```
ciscoasa# show controller
            pci
PCI Evaluation Log:
  ---------------------------------------------------------------------------
    Empty
  PCI Bus:Device.Function (hex): 00:00.0 Vendor ID: 0x8086 Device ID: 0x3406
  ---------------------------------------------------------------------------
    PCI Configuration Space (hex):
    0x00: 86 80 06 34 00 00 10 00 22 00 00 06 10 00 00 00
    0x10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x20: 00 00 00 00 00 00 00 00 00 00 00 00 86 80 00 00
    0x30: 00 00 00 00 60 00 00 00 00 00 00 00 05 01 00 00
    0x40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x60: 05 90 02 01 00 00 00 00 00 00 00 00 00 00 00 00
    0x70: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0x90: 10 e0 42 00 20 80 00 00 00 00 00 00 41 3c 3b 00
    0xa0: 00 00 41 30 00 00 00 00 c0 07 00 01 00 00 00 00
    0xb0: 00 00 00 00 3e 00 00 00 09 00 00 00 00 00 00 00
    0xc0: 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0xd0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    0xe0: 01 00 03 c8 08 00 00 00 00 00 00 00 00 00 00 00
    0xf0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    Link Capabilities: x4, Gen1
    Link Status: x4, Gen1
```

The following example is from ASA virtual. In this case, the rx_dropped_packets indicates that packets are being dropped at the VM level before entering the ASA virtual, possibly due to lack of bandwidth. One possible cause is that there is a blast/burst of traffic destined for the VM beyond what the VM can handle.

```
ciscoasa# show controller TenGigabitEthernet 0/2

TenGigabitEthernet0/2:
   DPDK Statistics
                  rx_good_packets : 13186640462
                  tx_good_packets : 3225386
                    rx_good_bytes : 12526548356100
                    tx_good_bytes : 383943970
                        rx_errors : 0
                        tx_errors : 0
         rx_mbuf_allocation_errors : 0
                     rx_q0packets : 0
                       rx_q0bytes : 0
                      rx_q0errors : 0
                     tx_q0packets : 0
                       tx_q0bytes : 0
                         rx_bytes : 12526548273860
               rx_unicast_packets : 13186630349
             rx_multicast_packets : 10025
             rx_broadcast_packets : 0
               rx_dropped_packets : 15357499
      rx_unknown_protocol_packets : 0
                         tx_bytes : 383943970
               tx_unicast_packets : 3224181
             tx_multicast_packets : 1205
             tx_broadcast_packets : 0
               tx_dropped_packets : 0
                 tx_error_packets : 0
```

Related Commands

Command	Description
show interface	Shows the interface statistics.
show tech-support	Shows information so Cisco TAC can diagnose problems.

show coredump filesystem

To show the contents of the coredump filesystem, enter the show coredump filesystem command.

show coredump filesystem

Syntax Description

This command has no arguments or keywords.

Command Default

By default, coredumps are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command shows the contents of the coredump filesystem.

Examples

To show the contents of any recent coredumps generated, enter the show coredump filesystem command.

```
ciscoasa(config)# show coredump filesystem
Coredump Filesystem Size is 100 MB
Filesystem type is FAT for disk0
Filesystem 1k-blocks Used Available Use% Mounted on
/dev/loop0 102182 75240 26942 74% /mnt/disk0/coredumpfsys
Directory of disk0:/coredumpfsys/
246 -rwx 20205386 19:14:53 Nov 26 2008 core_lina.2008Nov26_191244.203.11.gz
247 -rwx 36707919 19:17:27 Nov 26 2008 core_lina.2008Nov26_191456.203.6.gz
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change or affect the coredump configuration.

Command	Description
clear coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change/effect the coredump configuration.
show coredump log	Shows the coredump log.

show coredump log

To show the contents of the coredump log, newest first, enter the **show coredump log** command. To show the contents of the coredump log, oldest first, enter the **show coredump log reverse** command.

show coredump log
show coredump log [**reverse**]

Syntax Description

reverse	Shows the oldest coredump log.

Command Default

By default, coredumps are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

This command displays the contents of the coredump log. The logs should reflect what is currently on the disk.

Examples

The following example shows the output from these commands:

```
ciscoasa(config)# show coredump log
[ 1 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
[ 2 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump record
 'core_lina.2009Feb18_213558.203.11.gz'
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 5 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0'
```

Note The older coredump file is deleted to make room for the new coredump. This is done automatically by the ASA in the event the coredump filesystem fills and room is needed for the current coredump. This is why it is imperative to archive coredumps as soon as possible, to insure they don't get overwritten in the event of a crash.

ciscoasa(config)# show coredump log reverse

```
[ 1 ] Wed Feb 18 21:35:58 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_213558.203.11.gz' on 'disk0''
[ 2 ] Wed Feb 18 21:37:35 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_213558.203.11.gz', size 971722752 bytes, compressed size 21286383
[ 3 ] Wed Feb 18 22:10:32 2009: Coredump started for module 'lina', generating coredump
file 'core_lina.2009Feb18_221032.203.6.gz' on 'disk0'
[ 4 ] Wed Feb 18 22:11:01 2009: Filesystem full on 'disk0', removing module coredump record
 'core_lina.2009Feb18_213558.203.11.gz'
[ 5 ] Wed Feb 18 22:12:09 2009: Coredump completed for module 'lina', coredump file
'core_lina.2009Feb18_221032.203.6.gz', size 971722752 bytes, compressed size 21293688
```

Related Commands

Command	Description
coredump enable	Enables the coredump feature.
clear configure coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change/effect the coredump configuration.
clear coredump	Removes any coredumps currently stored on the coredump filesystem and clears the coredump log. Does not touch the coredump filesystem itself and does not change or affect the coredump configuration.
show coredump filesystem	Shows the contents of the coredump filesystem.

show counters

To display the protocol stack counters, use the **show counters** command in privileged EXEC mode.

show counters [**all** | **context** *context-name* | **summary** | top *N*] [**detail**] [**protocol** *protocol_name* [**:** *counter_name*]] [**threshold** *N*]

Syntax Description

all	Displays the filter details.
context *context-name*	Specifies the context name.
:*counter_name*	Specifies a counter by name.
detail	Displays additional counters information.
protocol *protocol_name*	Displays the counters for the specified protocol.
summary	Displays a counter summary.
threshold *N*	Displays only those counters at or above the specified threshold. The range is 1 through 4294967295.
top *N*	Displays the counters at or above the specified threshold. The range is 1 through 4294967295.

Command Default

show counters summary detail threshold 1

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.2(1)	Counters for the event manager were added.
9.13(1)	A new counter was added for the Firepower 1000 and 2100 in Appliance mode: HTTPERR: the number of HTTP request message timeouts to FXOS.

Release	Modification
9.12(1)	Five new counters were added for ACL search levels: • OBJGRP_SEARCH_THRESHOLD (Exceeding threshold 10000 search count) • OBJGRP_SEARCH_THRESHOLD_LEVEL4 (Between 7500 to 10000 searches) • OBJGRP_SEARCH_THRESHOLD_LEVEL3 (Between 5000 to 7500 searches) • OBJGRP_SEARCH_THRESHOLD_LEVEL2 (Between 2500 to 5000 searches) • OBJGRP_SEARCH_THRESHOLD_LEVEL1 (Between 1 to 2500 searches)

Examples

The following example shows how to display all counters:

```
ciscoasa#

show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf
ciscoasa# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
IP           OUT_PKTS            411   Summary
IP           TO_ARP              105   Summary
IP           TO_UDP                9   Summary
UDP          IN_PKTS               9   Summary
UDP          DROP_NO_APP           9   Summary
FIXUP        IN_PKTS             202   Summary
UAUTH        IPV6_UNSUPPORTED     27   Summary
IDFW         HIT_USER_LIMIT        2   Summary
```

The following example shows how to display a summary of counters:

```
ciscoasa#

show counters summary
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   Summary
IOS_IPC      OUT_PKTS              2   Summary
```

The following example shows how to display counters for a context:

```
ciscoasa# show counters context single_vf
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               4   single_vf
IOS_IPC      OUT_PKTS              4   single_vf
```

The following example shows how to display counters for the event manager:

```
ciscoasa# show counters protocol eem
Protocol     Counter           Value   Context
EEM          SYSLOG            22      Summary
EEM          COMMANDS           6       Summary
EEM          FILES              3       Summary
```

The following example shows how to display counters for ACL search levels:

```
ciscoasa# show counters
Protocol     Counter                                                                Value
   Context
ACL          OBJGRP_SEARCH_THRESHOLD                                       1582   Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL4                          534   Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL3                          524   Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL2                          307   Summary
ACL          OBJGRP_SEARCH_THRESHOLD_LEVEL1                          216   Summary
```

Related Commands

Command	Description
clear counters	Clears the protocol stack counters.

show cpu

To display the CPU utilization information, use the show cpu command in privileged EXEC mode.

[**cluster exec**] **show cpu** [**usage** *core-id* **| profile | dump | detailed**]

From the system configuration in multiple context mode:

[**cluster exec**] **show cpu** [**usage**] [**context** { **all** | *context_name* }]

Syntax Description

all	Specifies that the display show all contexts.
cluster exec	(Optional) In a clustering environment, enables you to issue the **show cpu** command in one unit and run the command in all the other units at the same time.
context	Specifies that the display show a context.
context_name	Specifies the name of the context to display.
core-id	Specifies the number of the processor core.
detailed	(Optional) Displays the CPU usage internal details.
dump	(Optional) Displays the dump profiling data to the TTY.
profile	(Optional) Displays the CPU profiling data.
usage	(Optional) Displays the CPU usage.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.6(1)	The *core-id* option was added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X.
9.1(2)	The output was updated for the **show cpu profile** and **show cpu profile dump** commands.
9.2(1)	Virtual platform CPU usage was added to the output for the ASA virtual.

Usage Guidelines

The CPU usage is computed using an approximation of the load every five seconds, and by further feeding this approximation into two, following moving averages.

You can use the **show cpu** command to find process related loads (that is, activity on behalf of items listed by the output of the **show process** command in both single mode and from the system configuration in multiple context mode).

Further, you can request, when in multiple context mode, a breakdown of the process related load to CPU consumed by any configured contexts by changing to each context and entering the **show cpu** command or by entering the **show cpu context** command.

While process related load is rounded to the nearest whole number, context related loads include one additional decimal digit of precision. For example, entering the **show cpu** command from the system context produces a different number than from entering the **show cpu context system** command. The former is an approximate summary of everything that appears in the **show cpu context all** command, and the latter is only a portion of that summary.

You can use the show cpu profile dump command in conjunction with the **cpu profile activate** command to collect information for TAC use in troubleshooting CPU issues. The **show cpu profile dump** command output is in hexadecimal format.

If the CPU profiler is waiting for a starting condition to occur, the **show cpu profile** command displays the following output:

```
CPU profiling started: 12:45:57.209 UTC Wed Nov 14 2012
CPU Profiling waiting on starting condition.
Core 0: 0 out of 10 samples collected.
Core 1: 0 out of 10 samples collected.
Core 2: 0 out of 10 samples collected.
Core 3: 0 out of 10 samples collected.
CP
0 out of 10 samples collected.
```

For the ASA virtual, note the following licensing guidelines:

- The number of allowed vCPUs is determined by the vCPU platform license installed.
  - If the number of licensed vCPUs matches the number of provisioned vCPUs, the state is Compliant.
  - If the number of licensed vCPUs is less than the number of provisioned vCPUs, the state is Noncompliant: Over-provisioned.
  - If the number of licensed vCPUs is more than the number of provisioned vCPUs, the state is Compliant: Under-provisioned.
- The memory limit is determined by the number of vCPUs provisioned.
  - If the provisioned memory is at the allowed limit, the state is Compliant.
  - If the provisioned memory is above the allowed limit, the state is Noncompliant: Over-provisioned.
  - If the provisioned memory is below the allowed limit, the state is Compliant: Under-provisioned.
- The Frequency Reservation limit is determined by the number of vCPUs provisioned.
  - If the frequency reservation memory is at or above the required minimum (1000 MHz), the state is Compliant.

- If the frequency reservation memory is below the required minimum (1000 MHz), the state is Compliant: Under-provisioned.

For example, the following output shows that no license has been applied. The number of allowed vCPUs refers to the number licensed, and Noncompliant: Over-provisioned indicates that the product is running with more resources than have been licensed.

```
Virtual platform CPU resources
------------------------------
Number of vCPUs              :        1
Number of allowed vCPUs      :        0
vCPU Status                  :        Noncompliant: Over-provisioned
```

Copy this information and provide it to the TAC for decoding.

Note When ASA is running on FXOS chassis, the number of CPU cores displayed in the **show cpu** command outputs may be less than the number displayed in the **show version** command output on some platforms, including Firepower 4100 and 9300 (FXOS-based) platforms.

The **show cpu** command output in Firepower 4100 and 9300 platforms has been modified due to the introduction of dynamic hyper-threading support. If the traffic throughput is low, the output in the **show cpu [detailed | core | external]** CLI is different, as seen with the standalone ASA output. If the CPU hyper-threading feature is disabled, the later part of the CPU core usage output is low. When the ASA traffic throughput is above the threshold limit, enabling the CPU hyper-threading feature results in the **show cpu** command displaying the same output as the standalone ASA.

Examples

The following example shows how to display the CPU utilization:

```
ciscoasa# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

The following example shows how to display detailed CPU utilization information. Note that the per core information is a sum of the (data path usage + control plane usage), as shown in parentheses.

```
ciscoasa# show cpu detailed
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  3.3 (0.0 + 3.3)  2.4 (0.0 + 2.4)
Current control point elapsed versus the maximum control point elapsed for:
      5 seconds = 99.0%; 1 minute: 99.8%; 5 minutes: 95.9%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
      5 seconds = 0.2%; 1 minute: 3.3%; 5 minutes: 2.5%
```

Note The “Current control point elapsed versus the maximum control point elapsed for” statement means that the current control point load is compared to the maximum load seen within the defined time period. This is a ratio instead of an absolute number. The figure of 99% for the 5-second interval means that the current control point load is at 99% of the maximum load that is visible over this 5-second interval. If the load continues to increase all the time, then it will always remain at 100%. However, the actual CPU may still have a lot of free capacity because the maximum absolute value has not been defined. Note that this number is not the sum of the "control plane usage" numbers for the cores.

The following example shows how to display the CPU utilization for the system context in multiple mode:

```
ciscoasa# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

The following example shows how to display the CPU utilization for all contexts:

```
ciscoasa# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

The following example shows how to display the CPU utilization for a context named “one”:

```
ciscoasa/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

The following example activates the profiler and instructs it to store 1000 samples.

```
ciscoasa# cpu profile activate
Activated CPU profiling for 1000 samples.
Use "show cpu profile" to display the progress or "show cpu profile dump" to interrupt
profiling and display the incomplete results.
```

The following examples show the status of the profiling (in-progress and completed):

```
ciscoasa# show cpu profile
CPU profiling started: 13:45:10.400 PST Fri Nov 16 2012
CPU profiling currently in progress:
Core 0: 209 out of 1000 samples collected.
Use "show cpu profile dump" to see the results after it is complete or to interrupt profiling
 and display the incomplete results.
ciscoasa# show cpu profile dump
Cisco Adaptive Security Appliance Software Version 9.1(2)
Hardware:   ASA5555
CPU profiling started: 09:13:32.079 UTC Wed Jan 30 2013
No CPU profiling process specified.
No CPU profiling trigger specified.
cores: 2
Process virtual address map:
---------------------------
...
---------------------------
End of process map
```

```
Samples for core 0 - stopped
{0x00000000007eadb6,0x000000000211ee7e} ...
```

The following example shows CPU usage for the ASA virtual:

```
ciscoasa# show cpu
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
Virtual platform CPU resources
------------------------------
Number of vCPUs              :     2
Number of allowed vCPUs      :     2
vCPU Status                  :  Compliant
Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  4000 MHz
Maximum allowed              :  56000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :   136 MHz
```

The following example shows details of CPU usage for the ASA virtual:

```
Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.2 (0.2 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.1 (0.0 + 0.1)  0.0 (0.0 + 0.0)
Current control point elapsed versus the maximum control point elapsed for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%
CPU utilization of external processes for:
     5 seconds = 0.0%; 1 minute: 0.0%; 5 minutes: 0.0%
Total CPU utilization for:
     5 seconds = 0.1%; 1 minute: 0.1%; 5 minutes: 0.1%
Virtual platform CPU resources
------------------------------
Number of vCPUs              :     4
Number of allowed vCPUs      :     4
vCPU Status                  :  Compliant
Frequency Reservation        :  1000 MHz
Minimum required             :  1000 MHz
Frequency Limit              :  20000 MHz
Maximum allowed              :  20000 MHz
Frequency Status             :  Compliant
Average Usage (30 seconds)   :    99 MHz
```

From ASA version 9.6.1, two or four cores are choosen for control point (CP) processing to limit the number of cores CP can run on, instead of letting CP float around all the available cores. Even if there is no traffic load, selected cores for CP processing has constant load for CPU pinning, which polls data path (DP) on each core for checking DP thread. This load is included in the **show cpu core** output, but excluded in the **show cpu detail** output because show cpu detail checks for CP and DP load.

Note On Secure Firewall 4200 series devices, core 0 is dedicated for control point, while the other cores are used to execute the data path processes.

Examples

The following example shows different CPU utilization values (Core 0 and Core 2) in the output of **show cpu core** and **show cpu detail** commands:

```
ciscoasa(config)# show cpu core
Core 5 sec 1 min 5 min
Core 0 18.0% 18.0% 18.0%
Core 1 0.0% 0.0% 0.0%
Core 2 18.6% 18.5% 18.6%
Core 3 0.0% 0.0% 0.0%
ciscoasa(config)# show cpu detail
Break down of per-core data path versus control point cpu usage:
Core 5 sec 1 min 5 min
Core 0 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6)
Core 1 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0)
Core 2 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6) 1.6 (0.0 + 1.6)
Core 3 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0) 0.0 (0.0 + 0.0)
```

Related Commands

Command	Description
show counters	Displays the protocol stack counters.
cpu profile activate	Activates CPU profiling.

show cr – show cz

show crashinfo

To display the contents of the latest crash information file stored in Flash memory, enter the **show crashinfo** command in privileged EXEC mode.

show crashinfo [**save**]

Syntax Description

save	(Optional) Displays if the ASA is configured to save crash information to Flash memory or not.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.1(5)	The output displays the thread ID (TID) in the **show process** command.
9.4(1)	The output displays the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.
9.7(1)	The output was updated to display only the latest system generated crash file.

Usage Guidelines

If the crash file is from a test crash (generated from the **crashinfo test** command), the first string of the crash file is "**: Saved_Test_Crash**" and the last string is "**: End_Test_Crash**". If the crash file is from a real crash, the first string of the crash file is "**: Saved_Crash**" and the last string is "**: End_Crash**". (This includes crashes from use of the **crashinfo force page-fault** or **crashinfo force watchdog** commands).

If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo** command displays an error message.

Note Crash information written to flash memory as a result of using **crashinfo test** command cannot be viewed in this command output. Only the real crash file displays in crashinfo_YYYYMMDD_HHMMSS 5_UTC format.

Examples

The following example shows how to display the current crash information configuration:

```
ciscoasa# show crashinfo save
crashinfo save enable
```

The following example shows the output for a crash file test. (However, this test does not actually crash the ASA. It provides a simulated example file.)

```
ciscoasa(config)# crashinfo test
ciscoasa(config)# exit
ciscoasa# show crashinfo
: Saved_Test_Crash
Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
F-flags  : 0x2
F-flags2 : 0x0
F-flags3 : 0x10000
F-flags4 : 0x0
F-bytes  : 0
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
```

```
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
```

```
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
```

```
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008
Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X
Compiled on Fri 15-Nov-04 14:35 by root
hostname up 10 days 0 hours
Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB
0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited
This XXX has a Restricted (R) license.
Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
```

```
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004
------------------ show clock ------------------
15:34:28.129 UTC Sun Nov 24 2004
------------------ show memory ------------------
Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes
------------------ show conn count ------------------
0 in use, 0 most used
------------------ show xlate count ------------------
0 in use, 0 most used
------------------ show vpn-sessiondb summary ------------------
Active Session Summary
Sessions:
                           Active : Cumulative : Peak Concurrent : Inactive
  SSL VPN               :       2 :          2 :               2
    Clientless only     :       0 :          0 :               0
    With client         :       2 :          2 :               2 :        0
  Email Proxy           :       0 :          0 :               0
  IPsec LAN-to-LAN      :       1 :          1 :               1
  IPsec Remote Access   :       0 :          0 :               0
  VPN Load Balancing    :       0 :          0 :               0
  Totals                :       3 :          3
License Information:
  Shared VPN License Information:
    SSL VPN                    :     1500
      Allocated to this device :       50
      Allocated in network     :       50
      Device limit             :      750
  IPsec   :    750    Configured :    750    Active :      1    Load :   0%
  SSL VPN :     52    Configured :     52    Active :      2    Load :   4%
                            Active : Cumulative : Peak Concurrent
  IPsec               :          1 :          1 :               1
  SSL VPN             :          2 :         10 :               2
    AnyConnect Mobile :          0 :          0 :               0
    Linksys Phone     :          0 :          0 :               0
  Totals              :          3 :         11
Tunnels:
                    Active : Cumulative : Peak Concurrent
  IKE         :          1 :          1 :               1
  IPsec       :          1 :          1 :               1
  Clientless  :          2 :          2 :               2
  SSL-Tunnel  :          2 :          2 :               2
  DTLS-Tunnel :          2 :          2 :               2
  Totals      :          8 :          8
------------------ show blocks ------------------
  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927
------------------ show interface ------------------
interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
------------------ show cpu usage ------------------
CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%
------------------ show process ------------------
PC  SP       STATE    Runtime  SBASE Stack              Process   TID
Hsi 001e3329 00763e7c 0053e5c8 0     00762ef4 3784/4096 arp_timer 0x000000000000000a
Lsi 001e80e9 00807074 0053e5c8 0     008060fc 3792/4096 FragDBGC  0x000000000000006b
Lwe 00117e3a 009dc2e4 00541d18         0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718         0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8         0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8         0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8         0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8         0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600         0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8         0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8         0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8         0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8         0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90         0 00d9b1c4 3944/4096 IPsec
Mwe 00205e25 00d9e1ec 0053e5c8         0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920         0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8         0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30         0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368         0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674         0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4         0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534      2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0      4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8         0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360         0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0         0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20         0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8         0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8         0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0         0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48       120 00f44344 3528/4096 ip/0:0
```

```
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA
------------------ show failover ------------------
No license for Failover
------------------ show traffic ------------------
outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
------------------ show perfmon ------------------
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

Related Commands

Command	Description
clear crashinfo	Deletes all the crash information files. the contents of the crash file.
crashinfo force	Forces a crash of the ASA.

Command	Description
crashinfo save disable	Disables crash information from writing to flash memory.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.
show crashinfo files	Displays the last five crash information files based on the date and timestamp.

show crashinfo console

To display the configuration setting of the **crashinfo console** command, enter the show crashinfo console command.

show crashinfo console

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(4)	This command was added.

Usage Guidelines

Compliance with FIPS 140-2 prohibits the distribution of Critical Security Parameters (keys, passwords, etc.) outside of the crypto boundary (chassis). When the device crashes, due to an assert or checkheaps failure, it is possible that the stack or memory regions dumped to the console contain sensitive data. This output must be suppressed in FIPS-mode.

Examples

```
sw8-5520(config)# show crashinfo console
crashinfo console enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
show running-config fips	Displays the FIPS configuration that is running on the ASA.

show crashinfo files

To display the latest system generated crash files in ASA, use the **show crashinfo files** command in privileged EXEC mode. The output displays a maximum of five crash files that are written to flash memory, based on the date and timestamp. The command output does not display any information if there are no crash files.

show crashinfo files

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Crash information written to flash memory as a result of using **crashinfo test** command cannot be viewed in **show crashinfo files** output. Only the real crash files display in crashinfo_YYYYMMDD_HHMMSS 5_UTC format. If there is no crash data saved in flash, or if the crash data has been cleared by entering the **clear crashinfo** command, the **show crashinfo files** command displays an error message.

Examples

The following example displays the actual crash information files:

```
ciscoasa# show crashinfo files
crashinfo_20160725_012315_UTC
crashinfo_20160725_021353_UTC
crashinfo_20160725_022309_UTC
crashinfo_20160725_024205_UTC
```

Related Commands

Command	Description
clear crashinfo	Deletes the contents of all the crash files.
crashinfo force	Forces the ASA to crash.
crashinfo save disable	Disables crash information from writing to flash memory.

Command	Description
show crashinfo	Displays the contents of the latest crash file.
crashinfo test	Tests the ability of the ASA to save crash information to a file in flash memory.

show crypto accelerator load-balance

To display the global and accelerator-specific load-balancing information from the hardware crypto accelerator MIB, use the **show crypto accelerator load-balance** command.

show crypto accelerator load-balance [**ipsec** | **ssl** | **detail** [**ipsec** | **ssl**]]

Syntax Description

detail	(Optional) Displays detailed information. You can include the ipsec or ssl keyword after this option.
ipsec	(Optional) Displays crypto accelerator IPSec load balancing details.
ssl	(Optional) Displays crypto accelerator SSL load balancing details.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto accelerator statistics

To display the global and accelerator-specific statistics from the hardware crypto accelerator MIB, use the **show crypto accelerator statistics** command in global configuration or privileged EXEC mode.

show crypto accelerator statistics

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The output statistics are defined as follows:

Accelerator 0 shows statistics for the software-based crypto engine.

Accelerator 1 shows statistics for the hardware-based crypto engine.

RSA statistics show RSA operations for 2048-bit keys, which are executed in software by default. This means that when you have a 2048-bit key, IKE/SSL VPN performs RSA operations in software during the IPsec/SSL negotiation phase. Actual IPsec/SSL traffic is still processed using hardware. This may cause high CPU if there are many simultaneous sessions starting at the same time, which may result in multiple RSA key operations and high CPU. If you run into a high CPU condition because of this, then you should use a 1024-bit key to process RSA key operations in hardware. To do so, you must reenroll the identity certificate. In releases 8.3(2) or later, you can also use the crypto engine large-mod-accel command on the 5510-5550 platforms to perform these operations in hardware.

If you are using a 2048-bit RSA key and the RSA processing is performed in software, you can use CPU profiling to determine which functions are causing high CPU usage. Generally, the bn_* and BN_* functions are math operations on the large data sets used for RSA, and are the most useful when examining CPU usage during an RSA operation in software. For example:

```
@@@@@@@@@@@@@@@@@@.............................. 36.50% : _bn_mul_add_words
@@@@@@@@@....................................... 19.75% : _bn_sqr_comba8
```

Diffie-Hellman statistics show that any crypto operation with a modulus size greater than 1024 is performed in software (for example, DH5 (Diffie-Hellman group 5 uses 1536)). If so, a 2048-bit key certificate will be processed in software, which can result in high CPU usage when a lot of sessions are running.

Note The ASA 5505 (with a Cavium CN505 processor) only supports Diffie-Hellman Groups 1 and 2 for hardware-accelerated, 768-bit and 1024-bit key generation. Diffie-Hellman Group 5 (1536-bit key generation) is performed in software.

A single crypto engine in the adaptive security appliance performs the IPsec and SSL operations. To display the versions of crypto (Cavium) microcode that are loaded into the hardware crypto accelerator at boot time, enter the **show version** command. For example:

```
ciscoasa(config) show version
Cisco Adaptive Security Appliance Software Version 8.0(4)8
Device Manager Version 6.1(5)
Compiled on Wed 15-Oct-09 17:27 by builders
System image file is "disk0:/interim/asa804-8-k8.bin"
Config file at boot was "startup-config"
asa up 5 days 17 hours
Hardware:   ASA5505, 512 MB RAM, CPU Geode 500 MHz
Internal ATA Compact Flash, 512MB
BIOS Flash M50FW080 @ 0xffe00000, 1024KB
Encryption hardware device : Cisco ASA-5505 on-board accelerator (revision 0x0)
                              Boot microcode   : CN1000-MC-BOOT-2.00
                              SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                              IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.05
```

DSA statistics show key generation in two phases. The first phase is a choice of algorithm parameters, which may be shared between different users of the system. The second phase computes private and public keys for a single user.

SSL statistics show records for the processor-intensive public key encryption algorithms involved in SSL transactions to the hardware crypto accelerator.

RNG statistics show records for a sender and receiver, which can generate the same set of random numbers automatically to use as keys.

Examples

The following example, entered in global configuration mode, shows global crypto accelerator statistics:

```
ciscoasa # show crypto accelerator statistics
Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
                             Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                             SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
```

The following table describes what the output entries indicates.

Output	**Description**
Capacity	This section pertains to the crypto acceleration that the ASA can support.
Supports hardware crypto	(True/False) The ASA can support hardware crypto acceleration.
Supports modular hardware crypto	(True/False) Any supported hardware crypto accelerator can be inserted as a separate plug-in card or module.
Max accelerators	The maximum number of hardware crypto accelerators that the ASA supports.
Mac crypto throughput	The maximum rated VPN throughput for the ASA.
Max crypto connections	The maximum number of supported VPN tunnels for the ASA.
Global Statistics	This section pertains to the combined hardware crypto accelerators in the ASA.
Number of active accelerators	The number of active hardware accelerators. An active hardware accelerator has been initialized and is available to process crypto commands.
Number of non-operational accelerators	The number of inactive hardware accelerators. An inactive hardware accelerator has been detected, but either has not completed initialization or has failed and is no longer usable.
Input packets	The number of inbound packets processed by all hardware crypto accelerators.

Output	Description
Input bytes	The number of bytes of data in the processed inbound packets.
Output packets	The number of outbound packets processed by all hardware crypto accelerators.
Output error packets	The number of outbound packets processed by all hardware crypto accelerators in which an error has been detected.
Output bytes	The number of bytes of data in the processed outbound packets.
Accelerator 0	Each of these sections pertains to a crypto accelerator. The first one (Accelerator 0) is always the software crypto engine. Although not a hardware accelerator, the ASA uses it to perform specific crypto tasks, and its statistics appear here. Accelerators 1 and higher are always hardware crypto accelerators.
Status	The status of the accelerator, which indicates whether the accelerator is being initialized, is active, or has failed.
Software crypto engine	The type of accelerator and firmware version (if applicable).
Slot	The slot number of the accelerator (if applicable).
Active time	The length of time that the accelerator has been in the active state.
Total crypto transforms	The total number of crypto commands that were performed by the accelerator.
Total dropped packets	The total number of packets that were dropped by the accelerator because of errors.
Input statistics	This section pertains to input traffic that was processed by the accelerator. Input traffic is considered to be ciphertext that must be decrypted and/or authenticated.
Input packets	The number of input packets that have been processed by the accelerator.
Input bytes	The number of input bytes that have been processed by the accelerator
Input hashed packets	The number of packets for which the accelerator has performed hash operations.
Input hashed bytes	The number of bytes over which the accelerator has performed hash operations.
Decrypted packets	The number of packets for which the accelerator has performed symmetric decryption operations.
Decrypted bytes	The number of bytes over which the accelerator has performed symmetric decryption operations.

Output	Description
Output statistics	This section pertains to output traffic that has been processed by the accelerator. Input traffic is considered clear text that must be encrypted and/or hashed.
Output packets	The number of output packets that have been processed by the accelerator.
Output bad packets	The number of output packets that have been processed by the accelerator in which an error has been detected.
Output bytes	The number of output bytes that have been processed by the accelerator.
Output hashed packets	The number of packets for which the accelerator has performed outbound hash operations.
Output hashed bytes	The number of bytes over which the accelerator has performed outbound hash operations.
Encyrpted packets	The number of packets for which the accelerator has performed symmetric encryption operations.
Encyrpted bytes	The number of bytes over which the accelerator has performed symmetric encryption operations.
Diffie-Hellman statistics	This section pertains to Diffie-Hellman key exchange operations.
Keys generated	The number of Diffie-Hellman key sets that have been generated by the accelerator.
Secret keys derived	The number of Diffie-Hellman shared secrets that have been derived by the accelerator.
RSA statistics	This section pertains to RSA crypto operations.
Keys generated	The number of RSA key sets that have been generated by the accelerator.
Signatures	The number of RSA signature operations that have been performed by the accelerator.
Verifications	The number of RSA signature verifications that have been performed by the accelerator.
Encrypted packets	The number of packets for which the accelerator has performed RSA encryption operations.
Decrypted packets	The number of packets for which the accelerator has performed RSA decryption operations.
Decrypted bytes	The number of bytes of data over which the accelerator has performed RSA decryption operations.
DSA statistics	This section pertains to DSA operations. Note that DSA is not supported as of Version 8.2, so these statistics are no longer displayed.

Output	Description
Keys generated	The number of DSA key sets that have been generated by the accelerator.
Signatures	The number of DSA signature operations that have been performed by the accelerator.
Verifications	The number of DSA signature verifications that have been performed by the accelerator.
SSL statistics	This section pertains to SSL record processing operations.
Outbound records	The number of SSL records that have been encrypted and authenticated by the accelerator.
Inbound records	The number of SSL records that have been decrypted and authenticated by the accelerator.
RNG statistics	This section pertains to random number generation.
Random number requests	The number of requests to the accelerator for a random number.
Random number request failures	The number of random number requests to the accelerator that did not succeed.

On platforms that support IPsec flow offload, the output shows the statistics for offloaded flows while the global counters show the total of all offloaded and non-offloaded flows for all accelerator engines on the device.

```
ciscoasa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supported TLS Offload Mode: HARDWARE
   Supports modular hardware crypto: False
   Max accelerators: 3
   Max crypto throughput: 3000 Mbps
   Max crypto connections: 3000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 108
   Input bytes: 138912
   Output packets: 118
   Output error packets: 0
   Output bytes: 142329

[Accelerator 0]
   Status: OK
   Software crypto engine
   Slot: 0
   Active time: 489 seconds
   Total crypto transforms: 2770
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
```

```
         Input bytes: 19232
         Input hashed packets: 0
         Input hashed bytes: 0
         Decrypted packets: 0
         Decrypted bytes: 19232
      [Output statistics]
         Output packets: 0
         Output bad packets: 0
         Output bytes: 18784
         Output hashed packets: 0
         Output hashed bytes: 0
         Encrypted packets: 0
         Encrypted bytes: 18784
      [Diffie-Hellman statistics]
         Keys generated: 0
         Secret keys derived: 0
      [RSA statistics]
         Keys generated: 1
         Signatures: 1
         Verifications: 1
         Encrypted packets: 1
         Encrypted bytes: 28
         Decrypted packets: 1
         Decrypted bytes: 256
      [ECDSA statistics]
         Keys generated: 13
         Signatures: 12
         Verifications: 15
      [EDDSA statistics]
         Keys generated: 0
         Signatures: 0
         Verifications: 0
      [SSL statistics]
         Outbound records: 0
         Inbound records: 0
      [RNG statistics]
         Random number requests: 0
         Random number request failures: 0
      [HMAC statistics]
         HMAC requests: 54

   [Accelerator 1]
      Status: OK
      Encryption hardware device : Cisco ASA Crypto on-board accelerator (revision 0x1)
                                   AE microcode        : CNN5x-MC-AE-MAIN-0007
                                   SE SSL microcode    : CNN5x-MC-SE-SSL-0018
      Slot: 1
      Active time: 497 seconds
      Total crypto transforms: 2910
      Total dropped packets: 0
      [Input statistics]
         Input packets: 4
         Input bytes: 13056
         Input hashed packets: 0
         Input hashed bytes: 0
         Decrypted packets: 4
         Decrypted bytes: 6528
      [Output statistics]
         Output packets: 14
         Output bad packets: 0
         Output bytes: 20786
         Output hashed packets: 0
         Output hashed bytes: 0
         Encrypted packets: 14
         Encrypted bytes: 10393
      [Offloaded Input statistics]
         Input packets: 106
         Input bytes: 115328
         Input hashed packets: 0
         Input hashed bytes: 0
         Decrypted packets: 107
         Decrypted bytes: 112992
      [Offloaded Output statistics]
         Output packets: 107
         Output bytes: 116416
         Output hashed packets: 0
         Output hashed bytes: 0
         Encrypted packets: 107
         Encrypted bytes: 112992
      Total dropped packets: 0
      [Diffie-Hellman statistics]
         Keys generated: 194
         Secret keys derived: 1
      [RSA statistics]
         Keys generated: 0
         Signatures: 2
         Verifications: 1
         Encrypted packets: 3
         Encrypted bytes: 162
         Decrypted packets: 2
         Decrypted bytes: 512
      [ECDSA statistics]
         Keys generated: 0
         Signatures: 0
         Verifications: 0
      [EDDSA statistics]
         Keys generated: 0
         Signatures: 0
         Verifications: 0
      [SSL statistics]
         Outbound records: 14
         Inbound records: 4
      [RNG statistics]
         Random number requests: 34
         Random number request failures: 0
      [HMAC statistics]
         HMAC requests: 26
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto protocol statistics	Displays the protocol-specific statistics from the crypto accelerator MIB.

show crypto ca certificates

To display the certificates associated with a specific trustpoint or to display all the certificates installed on the system, use the **show crypto ca certificates** command in global configuration or privileged EXEC mode.

show crypto ca certificates [*trustpointname*]

Syntax Description

trustpointname	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all certificates installed on the ASA.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show crypto ca certificates** command:

```
ciscoasa(config)# show crypto ca certificates test
Certificate
  Subject Name:
    commonName                = test
    unstructuredName          = ciscoasa.cisco.com
    serialNumber              = 9A8N02C5XFU
  Status: Pending terminal enrollment
  Key Usage: General Purpose
  Fingerprint:  7e2bb504 d8e2c4ca e45c76af 5309d2e4
  Associated Trustpoint: test
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.

Command	Description
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint configuration mode for a specified trustpoint.

show crypto ca crl

To display all cached CRLs or to display all CRLs cached for a specified trustpoint, use the **show crypto ca crl** command in global configuration or privileged EXEC mode.

show crypto ca crl [**trustpool** | **trustpoint** *<trustpointname>*]

Syntax Description

trustpoint *trustpointname*	(Optional) The name of a trustpoint. If you do not specify a name, this command displays all CRLs cached on the ASA.
trustpool	The name of the trust pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show crypto ca crl** command:

```
ciscoasa(config)# show crypto ca crl tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@example.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Obtains a CA certificate for a specified trustpoint.

Command	Description
crypto ca crl request	Requests a CRL based on the configuration parameters of a specified trustpoint.
crypto ca enroll	Initiates the enrollment process with a CA.
crypto ca import	Imports a certificate to a specified trustpoint.
crypto ca trustpoint	Enters trustpoint configuration mode for a specified trustpoint.

show crypto ca server

To display the status of the local CA configuration on the ASA, use the **show crypto ca server** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following is sample output from the **show crypto ca server** command:

```
ciscoasa# show crypto ca server
#Certificate Server LOCAL-CA-SERVER:
    Status: disabled
    State: disabled
    Server's configuration is unlocked (enter "no shutdown" to lock it)
    Issuer name: CN=asa1.cisco.com
    CA cert fingerprint: -Not found-
    Last certificate issued serial number: 0x0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 2009
    CRL not present.
    Current primary storage dir: nvram:
ciscoasa#
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
debug crypto ca server	Shows debugging messages when you configure the local CA server.
show crypto ca server certificate	Displays the certificate of the local CA in base64 format.
show crypto ca server crl	Displays the lifetime of the local CA CRL.

show crypto ca server cert-db

To display all or a subset of local CA server certificates, including those issued to a specific user, use the **show crypto ca server cert-db** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server cert-db [**username** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]

Syntax Description

allowed	Specifies that users who are allowed to enroll appear, regardless of the status of their certificate.
enrolled	Specifies that users with valid certificates appear.
expired	Specifies that users holding expired certificates appear.
on-hold	Specifies that users who have not yet enrolled appear.
serial certificate-serial-number	Specifies the serial number of a specific certificate that displays. The serial number must be in hexadecimal format.
username username	Specifies the certificate owner. The username may be a username or an e-mail address. For e-mail addresses, it is the e-mail address used to contact and deliver the one-time password (OTP) to the end user. An e-mail address is required to enable e-mail notifications for the end user.

Command Default

By default, if no username or certificate serial number is specified, the entire database of issued certificates appears.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **show crypto ca server cert-db** command displays a list of the user certificates that are issued by the local CA server. You can display a subset of the certificate database by specifying a specific username with one or more of the optional certificate-type keywords, and/or with an optional certificate serial number.

If you specify a username without a keyword or a serial number, all of the certificates issued for that user appear. For each user, the output shows the username, e-mail address, domain name, the time period for which enrollment is allowed, and the number of times that the user has been notified with an enrollment invitation.

In addition, the following information appears in the output:

- The NOTIFIED field is required to support multiple reminders. It tracks when a user needs to be notified of the OTP for enrollment and the reminder notification attempts. This field is set to 0 initially. It is incremented to 1 when the user entry is marked as being allowed to enroll. At this time, the initial OTP notification is generated.
- The NOTIFY field is incremented each time a reminder is sent. Three notifications are sent before the OTP is due to expire. A notification is sent when the user is allowed to enroll, at the mid-point of the expiration, and when ¾ of the expiration time has passed. This field is used only for administrator-initiated enrollments. For automatic certificate renewals, the NOTIFY field in the certificate database is used.

Note While the notification counter in this command is used to track the number of times a user is notified to renew a certificate before expiration, the notification counter in show crypto ca server user-db is used to track the number of times a user is notified to enroll for the certificate. Renewal notifications are tracked under cert-db and not included in user-db.

Each certificate displays the certificate serial number, the issued and expired dates, and the certificate status (Revoked/Not Revoked).

Examples

The following example requests the display of all of the certificates issued for ASA by the CA server:

```
ciscoasa# show crypto ca server cert-db username asa
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

The following example requests the display of all the certificates issued by the local CA server with a serial number of 0x2:

ciscoasa# **show crypto ca server cert-db serial 2**

```
Username:asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
```

```
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

The following example requests the display of all of the certificates issued by the local CA server:

```
ciscoasa# show crypto ca server cert-db
Username: asa
Renewal allowed until: Not Allowed
Number of times user notified: 0
PKCS12 file stored until: 10:28:05 UTC Wed Sep 25 2013
Certificates Issued:
serial:   0x2
issued:   10:28:04 UTC Tue Sep 24 2013
expired:  10:28:04 UTC Thu Sep 26 2013
status:   Not Revoked
```

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in both the certificate database and CRL.
lifetime crl	Specifies the lifetime of the CRL.

show crypto ca server certificate

To display the certificate for the local CA server in base64 format, use the **show crypto ca server certificate** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server certificate

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **show crypto ca server certificate** command displays the local CA server certificate in base64 format. This display allows you to cut and paste a certificate while exporting it to other devices that need to trust the local CA server.

Examples

The following is sample output from the **show crypto ca server certificate** command:

```
ciscoasa# show crypto ca server certificate
The base64 encoded local CA certificate follows:
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+
MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAM
IIXHAYJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQ
Ijph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphs
UM+IG3SDOiDwZG9n1SvtMieoxd7Hxknxbum06JDruj
WKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzw
cRhl1KEZTS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeL
j3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwP
EdPQxaWZPrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3
Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d
5nlOiJjDYYbP86tvbZ2yOVZR6aKFVI0b2AfCr6Pbw
```

```
fC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA
5KWScyEcgdqmuBeGDKOncTknfgy0XM+fG5rb3qAXy1
GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj....
```

ciscoasa#

Related Commands

Command	Description
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage a local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
keysize	Specifies the size of the public and private keys generated at user certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate and issued certificates.
show crypto ca server	Displays the local CA configuration in ASCII text format.

show crypto ca server crl

To display the current CRL of the local CA, use the **show crypto ca server crl** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server crl

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following is sample output from the **show crypto ca server crl** command:

```
ciscoasa
# show crypto ca server crl
asa5540(config)# sh cry ca ser crl
Certificate Revocation List:
    Issuer: cn=asa5540.frqa.cisco.com
    This Update: 07:32:27 UTC Oct 16 2006
    Next Update: 13:32:27 UTC Oct 16 2006
    Number of CRL entries: 0
    CRL size: 232 bytes
asa5540(config)#
ciscoasa
#
```

Related Commands

Command	Description
cdp-url	Specifies the CRL distribution point (CDP) to be included in the certificates issued by the CA.
crypto ca server	Provides access to the ca server configuration mode CLI command set, which allows you to configure and manage the local CA.
crypto ca server revoke	Marks a certificate issued by the local CA server as revoked in the certificate database and CRL.
lifetime crl	Specifies the lifetime of the CRL.
show crypto ca server	Displays the status of the CA configuration.

show crypto ca server user-db

To display users included in the local CA server user database, use the **show crypto ca server user-db** command in ca server configuration, global configuration, or privileged EXEC mode.

show crypto ca server user-db [**expired** | **allowed** | **on-hold** | **enrolled**]

Syntax Description

allowed	(Optional) Specifies that users who are allowed to enroll display, regardless of the status of their certificate.
enrolled	(Optional) Specifies that users with valid certificates display.
expired	(Optional) Specifies that users holding expired certificates display.
on-hold	(Optional) Specifies that users who have not enrolled yet display.

Command Default

By default, all users in the database display if no keywords are entered.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example displays currently enrolled users:

```
ciscoasa# show
            crypto ca server user-db enrolled
Username   DN     Certificate issued      Certificate expiration
exampleuser  cn=Example User,o=...     5/31/2009       5/31/2010
ciscoasa#
```

Usage Guidelines

While the notification counter in this command is used to track the number of times a user is notified to enroll for the certificate, the notification counter in show crypto ca server cert-db is used to track the number of times a user is notified to renew a certificate before expiration. Renewal notifications are tracked under cert-db and not included in user-db.

Related Commands

Command	Description
crypto ca server user-db add	Adds a user to the CA server user database.
crypto ca server user-db allow	Allows a specific user or a subset of users in the CA server database to enroll with the local CA.
crypto ca server user-db remove	Removes a user from the CA server user database.
crypto ca server user-db write	Writes user information configured in the local CA database to storage.
show crypto ca server cert-db	Displays all certificates issued by the local CA.

show crypto ca trustpool

To display the certificates that constitute the trustpool, use the **show crypto ca trustpool** command in privileged EXEC mode.

show crypto ca trustpool [**detail**]

Syntax Description

This command has no arguments or keywords.

Command Default

This command shows an abbreviated display of all the trustpool certificates. When the “detail” option is specified, more information is included.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The output of the show crypto ca trustpool command includes the fingerprint value of each certificate. These values are required for removal operation.

Examples

```
ciscoasa# show crypto ca trustpool
CA Certificate
Status: Available
Certificate Serial Number: 6c386c409f4ff4944154635da520ed4c
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name: cn=bxb2008-root
dc=bdb2008
dc=mycompany
dc=com
Subject Name:
cn=bxb2008-root
dc=bxb2008
dc=cisco
dc=com
Validity Date:
start date:17:21:06 EST Jan 14 2009
end date:17:31:06 EST Jan 14 2024
CA Certificate
Status: Available
```

```
Certificate Serial Number: 58d1c756000000000059
Certificate Usage: Signature
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=bxb2008-root
dc=bxb2008
dc=mycompany
dc=com
Subject Name:
cn=BXB2008SUB1-CA
dc=bxb2008
dc=cisco
dc=com
OCSP AIA:
URL: http://bxb2008-1.bxb2008.mycompany.com/ocsp
CRL Distribution Points:
(1) http://bxb2008-1.bxb2008.mycompany.com/CertEnroll/bxb2008-root.crl
Validity Date:
start date:11:54:34 EST May 18 2009
end date:12:04:34 EST May 18 2011
```

Related Commands

Command	Description
clear crypto ca trustpool	Removes all certificates from the trustpool.
crypto ca trustpool import	Imports certificates that constitute the PKI trustpool.
crypto ca trustpool remove	Removes a single specified certificate from the trustpool.

show crypto ca trustpool policy

To display the configured trustpool policy and process any applied certificate maps to show how those impact the policy, use the **show crypto ca trustpool policy** command in privileged EXEC mode.

show crypto ca trustpool policy

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.
9.5(2)	The ability to show status and results of automatic import of trustpool certificates was added.

Examples

```
ciscoasa(config)# sh run cry ca cert map
crypto ca certificate map map1 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca
crypto ca certificate map map 2 1
issuer-name eq cn = mycompany manufacturing ca
issuer-name eq cn = mycompany ca2
ciscoasa(config)#
ciscoasa(config)# sh run crypto ca trustpool policy
crypto ca trustpool policy
auto-import url http://www.thawte.com
revocation-check none
match certificate map2 allow expired-certificate
match certificate map1 skip revocation-check
crl cache-time 123
crl enforcenextupdate
auto-import
auto-import url http://www.thawte.com
auto-import time 22:00:00
ciscoasa(config)#
ciscoasa# show crypto ca trustpool policy
800 trustpool certificates installed
Trustpool auto import statistics:
 Last import result: SUCCESS
 Next scheduled import at 22:00:00 Tues Jul 21 2015
Trustpool Policy
Trustpool revocation checking is disabled
CRL cache time: 123 seconds
CRL next update field: required and forced
Automatic import of trustpool certificates is enabled
Automatic import URL: http://www.thawte.com
Download time: 22:00:00
Policy overrides:
map: map1
match:issuer-name eq cn=Mycompany Manufacturing CA
match:issuer-name eq cn=Mycompany CA
action:skip revocation-check
map: map2
match: issuer-name eq cn=mycompany Manufacturing CA
match: issuer-name eq cn=mycompany CA2
action: allowed expired certificates
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ca trustpool policy	Enters a submode that provides the commands that define the trustpool policy.

show crypto debug-condition

To display the currently configured filters, the unmatched states, and the error states for IPsec and ISAKMP debugging messages, use the **show crypto debug-condition** command in global configuration mode.

show crypto debug-condition

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example shows the filtering conditions:

```
ciscoasa(config)# show crypto debug-condition
Crypto conditional debug is turned ON
IKE debug context unmatched flag:  OFF
IPsec debug context unmatched flag:  ON
IKE peer IP address filters:
1.1.1.0/24   2.2.2.2
IKE user name filters:
my_user
```

Related Commands

Command	Description
debug crypto condition	Sets filtering conditions for IPsec and ISAKMP debugging messages.
debug crypto condition error	Shows debugging messages whether or not filtering conditions have been specified.
debug crypto condition unmatched	Shows debugging messages for IPsec and ISAKMP that do not include sufficient context information for filtering.

show crypto ikev1 sa

To display the IKEv1 runtime SA database, use the **show crypto ikev1 sa** command in global configuration mode or privileged EXEC mode.

show crypto ikev1 sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
ciscoasa(config)# show crypto ikev1 sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
ciscoasa(config)#
```

Related Commands

Command	Description
show crypto ikev2 sa	Displays the IKEv2 runtime SA database.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto ikev2 sa

To display the IKEv2 runtime SA database, use the **show crypto ikev2 sa** command in global configuration mode or privileged EXEC mode.

show crypto ikev2 sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.19(1)	Dual-stack support for IKEv2 third-party clients is added. Number of traffic selectors that a child SA can store is extended to 2 traffic selectors.
9.20(1)	Multiple key exchanges for IKEv2 policy.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
ciscoasa(config)# show crypto ikev2 sa detail
IKEv2 SAs:
Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id                 Local                Remote     Status         Role
671069399        10.0.0.0/500 10.255.255.255/500      READY    INITIATOR
      Encr: AES-GCM, keysize: 256, Hash: N/A, DH Grp:20, Auth sign: PSK, Auth verify: PSK
      Additional Key Exchange Group: AKE1: 31 AKE2: 21 AKE3: 20 AKE4: 19 AKE5: 16 AKE6: 15
 AKE7: 14
      Life/Active Time: 86400/188 sec
      Session-id: 1
      Status Description: Negotiation done
      Local spi: 80173A0373C2D403       Remote spi: AE8AEFA1B97DBB22
      Local id: asa
      Remote id: asa1
      Local req mess id: 8              Remote req mess id: 7
      Local next mess id: 8             Remote next mess id: 7
      Local req queued: 8               Remote req queued: 7
      Local window: 1                   Remote window: 1
      DPD configured for 10 seconds, retry 2
      NAT-T is not detected
      Mobile is enabled
      Assigned host addr: 192.168.0.12
      Assigned host addr IPv6: 2001:db8::2
      IKEv2 Fragmentation Configured MTU:576 bytes, Overhead: 28 bytes, Effective MTU: 548
 bytes
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
                          ::/0- ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:/65535
          remote selector 192.186.0.12/0 - 192.186.0.12/65535
                          2001:db8::2/0- 2001:db8::2/65535
          ESP spi in/out: 0x242a3da5/0xe6262034
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-GCM, keysize: 128, esp_hmac: N/A
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

Related Commands

Command	Description
show crypto ikev1 sa	Displays the IKEv1 runtime SA database.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto ikev2 stats

To display the IKEv2 runtime statistics use the **show crypto ikev2 stats** command in global configuration mode or privileged EXEC mode.

show crypto ikev2 stats

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.9(1)	Local IKEv2 statistics are now provided

Usage Guidelines

The local output from this command is:

```
Global IKEv2 Statistics
  Active Tunnels:                          0
  Previous Tunnels:                        0
  In Octets:                               0
  In Packets:                              0
  In Drop Packets:                         0
  In Drop Fragments:                       0
  In Notifys:                              0
  In P2 Exchange:                          0
  In P2 Exchange Invalids:                 0
  In P2 Exchange Rejects:                  0
  In IPSEC Delete:                         0
  In IKE Delete:                           0
  Out Octets:                              0
  Out Packets:                             0
  Out Drop Packets:                        0
  Out Drop Fragments:                      0
  Out Notifys:                            0
  Out P2 Exchange:                        0
  Out P2 Exchange Invalids:               0
  Out P2 Exchange Rejects:                0
  Out IPSEC Delete:                       0
  Out IKE Delete:                         0
  SAs Locally Initiated:                  0
  SAs Locally Initiated Failed:           0
  SAs Remotely Initiated:                 0
  SAs Remotely Initiated Failed:          0
  System Capacity Failures:               0
  Authentication Failures:                0
  Decrypt Failures:                       0
  Hash Failures:                          0
  Invalid SPI:                            0
  In Configs:                             0
  Out Configs:                            0
  In Configs Rejects:                     0
  Out Configs Rejects:                    0
  Previous Tunnels:                       0
  Previous Tunnels Wraps:                 0
  In DPD Messages:                        0
  Out DPD Messages:                       0
  Out NAT Keepalives:                     0
  IKE Rekey Locally Initiated:            0
  IKE Rekey Remotely Initiated:           0
  Locally Initiated IKE Rekey Rejected:   0
  Remotely Initiated IKE Rekey Rejected:  0
  CHILD Rekey Locally Initiated:          0
  CHILD Rekey Remotely Initiated:         0

IKEV2 Call Admission Statistics
  Max Active SAs:                  No Limit
  Max In-Negotiation SAs:             15000
  Cookie Challenge Threshold:         Never
  Active SAs:                             0
  In-Negotiation SAs:                     0
  Incoming Requests:                      0
 Incoming Requests Accepted:            0
  Incoming Requests Rejected:             0
  Outgoing Requests:                      0
  Outgoing Requests Accepted:             0
  Outgoing Requests Rejected:             0
  Rejected Requests:                      0
  Rejected Over Max SA limit:             0
  Rejected Low Resources:                 0
  Rejected Reboot In Progress:            0
  Cookie Challenges:                      0
  Cookie Challenges Passed:               0
  Cookie Challenges Failed:               0
```

Related Commands

Command	Description
show crypto ikev2 sa	Displays the IKEv1 runtime SA database.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto ipsec df-bit

To display the IPsec do-not-fragment (DF-bit) policy for IPsec packets for a specified interface, use the **show crypto ipsec df-bit** command in global configuration mode and privileged EXEC mode. You can also use the command synonym **show ipsec df-bit**.

show crypto ipsec df-bit *interface*

Syntax Description

interface	Specifies an interface name.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The df-bit setting determines how the system handles the do-not-fragment (DF) bit in the encapsulated header. The DF bit within the IP header determines whether or not a device is allowed to fragment a packet. Based on this setting, the system either clears, sets, or copies the DF-bit setting of the clear-text packet to the outer IPsec header when applying encryption.

Examples

The following example displays the IPsec DF-bit policy for interface named inside:

```
ciscoasa(config)# show
 crypto
 ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the IPsec DF-bit policy for IPsec packets.

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
show crypto ipsec fragmentation	Displays the fragmentation policy for IPsec packets.

show crypto ipsec fragmentation

To display the fragmentation policy for IPsec packets, use the **show crypto ipsec fragmentation** command in global configuration or privileged EXEC mode. You can also use the command synonym **show ipsec fragmentation**.

show crypto ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When encrypting packets for a VPN, the system compares the packet length with the MTU of the outbound interface. If encrypting the packet will exceed the MTU, the packet must be fragmented. This command shows whether the system will fragment the packet after encrypting it (after-encryption), or before encrypting it (before-encryption). Fragmenting the packet before encryption is also called prefragmentation, and is the default system behavior because it improves overall encryption performance.

Examples

The following example, entered in global configuration mode, displays the IPsec fragmentation policy for an interface named inside:

```
ciscoasa(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPsec packets.

Command	Description
show crypto ipsec df-bit	Displays the DF-bit policy for a specified interface.

show crypto ipsec policy

To display IPsec secure socket API (SS API) security policy configured for OSPFv3, use the **show crypto ipsec policy** command in global configuration or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec policy**.

show crypto ipsec policy

Syntax Description

This command has no keywords or variables.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows the OSPFv3 authentication and encryption policy.

```
ciscoasa# show crypto ipsec policy

Crypto IPsec client security policy data
Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   1234567890123456789012345678901234567890
Outbound ESP Auth Key:   1234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 12345678901234567890123456789012
Outbound ESP Cipher Key: 12345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

Command	Description
ipv6 ospf encryption	Configures the authentication and encryption policy for OSPFv3.
show crypto sockets	Displays secure socket information.

Command	Description
show ipv6 ospf interface	Displays information about OSPFv3 interfaces.

show crypto ipsec sa

To display a list of IPsec SAs, use the **show crypto ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show ipsec sa** .

show crypto ipsec sa [**entry | identity | map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description

detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPsec SAs sorted by peer address
identity	(Optional) Displays IPsec SAs for sorted by identity, not including ESPs. This is a condensed form.
map *map-name*	(Optional) Displays IPsec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPsec SAs for specified peer IP addresses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for OSPFv3, multiple context mode, Suite B algorithm in the transform and IV size portion, and ESPV3 IPsec output were added.
9.13(1)	The following new counters was added for troubleshooting errors in *show crypto ipsec sa detail* : • **#pkts invalid ip version (send)** • **#pkts invalid length (send)** • **#pkts invalid ctx (send) and #pkts invalid ctx (rcv)** • **#pkts invalid ifc (send) and #pkts invalid ifc (rcv)** • **#pkts failed (send) and #pkts failed (rcv)**

Release	Modification
9.19(1)	Dual-stack support for IKEv2 third-party clients is added. Number of traffic selectors that inbound and outbound IPsec SA can support is extended to 2 traffic selectors.

Examples

The following example, entered in global configuration mode, displays IPsec SAs that include a tunnel identified as OSPFv3.

```
ciscoasa(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key, (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

Note Fragmentation statistics are pre-fragmentation statistics if the IPsec SA policy states that fragmentation occurs before IPsec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPsec processing.

```
The following example, entered in global configuration mode, shows IPsec SAs for the keyword
 detail with the newly added counters to troubleshoot the errors in the traffic.
(config)# sh ipsec sa det
interface: outside
```

```
Crypto map tag: outside_map, seq num: 10, local addr: 10.86.94.103
  access-list toASA-5525 extended permit ip host 10.86.94.103 host 10.86.95.135
  local ident (addr/mask/prot/port): (10.86.94.103/255.255.255.255/0/0)
  remote ident (addr/mask/prot/port): (10.86.95.135/255.255.255.255/0/0)
  local ident (addr/mask/prot/port): (::/0/0/0)
  remote ident (addr/mask/prot/port): (3000::1/128/0/0)
  current_peer: 10.86.95.135
  dynamic allocated peer ip: 10.86.95.135
  dynamic allocated peer ip(ipv6): 3000::1
  #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
  #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp failed: 0
  #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
  #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
  #TFC rcvd: 0, #TFC sent: 0
  #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
  #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
  #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
  #pkts invalid prot (rcv): 0, #pkts verify failed: 0
  #pkts invalid identity (rcv): 0
  #pkts invalid pad (rcv): 0
  #pkts invalid ip version (send): 0, #pkts invalid ip version (rcv): 0
  #pkts invalid len (send): 0, #pkts invalid len (rcv): 0
  #pkts invalid ctx (send): 0, #pkts invalid ctx (rcv): 0
  #pkts invalid ifc (send): 0, #pkts invalid ifc (rcv): 0
  #pkts failed (send): 0, #pkts failed (rcv): 0
  #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
  #pkts replay failed (rcv): 0
  #pkts min mtu frag failed (send): 0, #pkts bad frag offset (rcv): 0
  #pkts internal err (send): 0, #pkts internal err (rcv): 0

  local crypto endpt.: 10.86.94.103/500, remote crypto endpt.: 10.86.95.135/500
  path mtu 1500, ipsec overhead 94(44), media mtu 1500
  PMTU time remaining (sec): 0, DF policy: copy-df
  ICMP error validation: disabled, TFC packets: disabled
  current outbound spi: 25356578
  current inbound spi : A1029CE2
inbound esp sas:
  spi: 0xA1029CE2 (2701303010)
     SA State: active
     transform: esp-aes esp-sha-512-hmac no compression
     in use settings ={L2L, Tunnel, IKEv2, }
     slot: 0, conn_id: 195272704, crypto-map: outside_map
     sa timing: remaining key lifetime (kB/sec): (3962879/28782)
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
      0x00000000 0x0000001F
outbound esp sas:
  spi: 0x25356578 (624256376)
     SA State: active
     transform: esp-aes esp-sha-512-hmac no compression
     in use settings ={L2L, Tunnel, IKEv2, }
     slot: 0, conn_id: 195272704, crypto-map: outside_map
     sa timing: remaining key lifetime (kB/sec): (4193279/28772)
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
     0x00000000 0x00000001
```

The following example, entered in global configuration mode, displays IPsec SAs for a crypto map named def.

```
ciscoasa(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

The following example, entered in global configuration mode, shows IPsec SAs for the keyword **entry** .

```
ciscoasa(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 212
          IV size: 8 bytes
          replay detection support: Y
     outbound esp sas:
       spi: 0x3B6F6A35 (997157429)
          transform: esp-3des esp-md5-hmac
          in use settings ={RA, Tunnel, }
          slot: 0, conn_id: 4, crypto-map: def
          sa timing: remaining key lifetime (sec): 212
          IV size: 8 bytes
          replay detection support: Y
ciscoasa(config)#
```

The following example, entered in global configuration mode, shows IPsec SAs with the keywords **entry detail** .

```
ciscoasa(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

The following example shows IPsec SAs with the keyword **identity** .

```
ciscoasa(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8::1
      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPsec SAs with the keywords **identity** and **detail** .

```
ciscoasa(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3000::1/128/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      dynamic allocated peer ip(ipv6): 3000::1
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      local ident (addr/mask/prot/port): (::/0/0/0)
      remote ident (addr/mask/prot/port): (3001:db8::1/128/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      dynamic allocated peer ip(ipv6): 3001:db8:1
      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config isakmp	Displays all the active ISAKMP configuration.

show crypto ipsec stats

To display a list of IPsec statistics, use the **show crypto ipsec stats** command in global configuration mode or privileged EXEC mode.

show crypto ipsec stats

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example, entered in global configuration mode, displays IPsec statistics:

```
ciscoasa(config)# show crypto ipsec stats
IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
```

```
      Authentications: 74029
      Authentication failures: 0
      Encryptions: 74029
      Encryption failures: 0
   Fragmentation successes: 3
    Pre-fragmentation successes:2
    Post-fragmentation successes: 1
   Fragmentation failures: 2
    Pre-fragmentation failures:1
    Post-fragmentation failures: 1
   Fragments created: 10
   PMTUs sent: 1
   PMTUs recvd: 2
  Protocol failures: 0
  Missing SA failures: 0
  System capacity failures: 0
  ciscoasa(config)#
```

Related Commands

Command	Description
clear ipsec sa	Clears IPsec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPsec SAs.

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
```

```
No Sa Fails: 0
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp sa

To display the IKE runtime SA database, use the **show crypto isakmp sa** command in global configuration mode or privileged EXEC mode.

show crypto isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp sa** command was added.
7.2(1)	This **show isakmp sa** command was deprecated. The **show crypto isakmp sa** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified

IKE Peer 209.165.200.225

Type—L2L or User

Dir—Init

Rky—No or Yes. If yes, a rekey is occurring, and a second matching SA will be in a different state until the rekey completes.

Role—Initiator or Responder State. Tells the current state of the state machine for the SA.

State—A tunnel up and passing data has a value of either MM_ACTIVE or AM_ACTIVE. Other active states include MM_BLD_MSG4, MM_BLD_MSG6, MM_FREE, MM_SND_MSG6_H, MM_START, MM_TM_INIT_MODECFG_H, MM_TM_PEND_QM, MM_WAIT_DELETE, MM_WAIT_MSG3, MM_WAIT_MSG5, and so on.

Detail specified

IKE Peer 209.165.200.225

Type—L2L or User

Dir—Init

Rky—No or Yes. If yes, a rekey is occurring, and a second matching SA will be in a different state until the rekey completes.

Role—Initiator or Responder State. Tells the current state of the state machine for the SA. A tunnel up and passing data has a value of either MM_ACTIVE or AM_ACTIVE.

State—Other than MM_ACTIVE or AM_ACTIVE, other active states include MM_BLD_MSG4, MM_BLD_MSG6, MM_FREE, MM_SND_MSG6_H, MM_START, MM_TM_INIT_MODECFG_H, MM_TM_PEND_QM, MM_WAIT_DELETE, MM_WAIT_MSG3, MM_WAIT_MSG5, and so on.

Encrypt—3des

Hash—md5

Auth—preshrd

Lifetime—86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
ciscoasa(config)# show crypto isakmp sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto isakmp stats

To display runtime statistics, use the **show crypto isakmp stats** command in global configuration mode or privileged EXEC mode.

show crypto isakmp stats

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	The **show isakmp stats** command was added.
7.2(1)	The **show isakmp stats** command was deprecated. The **show crypto isakmp stats** command replaced it.

Usage Guidelines

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests

- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
ciscoasa(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
```

```
No Sa Fails: 0
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show crypto key mypubkey

To display the default keys (called "mypubkey") and information about the keys, use the **show crypto key mypubkey** command in privileged EXEC mode.

show crypto key mypubkey { **ecdsa** | **eddsa** | **rsa** }

Syntax Description

ecdsa	Specifies the key type as ECDSA.
eddsa	Specifies the key type as EDDSA.
rsa	Specifies the key type as RSA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for ECDSA keys was added.
9.16(1)	Support for EDDSA keys was added.

Related Commands

Command	Description
cryto key generate	Creates key pairs.
crypto key zeroize	Removes key pairs.

show crypto protocol statistics

To display the protocol-specific statistics in the crypto accelerator MIB, use the **show crypto protocol statistics** command in global configuration or privileged EXEC mode.

show crypto protocol statistics *protocol*

Syntax Description

protocol	Specifies the name of the protocol for which to display statistics. Protocol choices are as follows: **ikev1**—Internet Key Exchange version 1. **ipsec**—IP Security Phase-2 protocols. **ssl**—Secure Sockets Layer. **other**—Reserved for new protocols. **all**—All protocols currently supported.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following examples entered in global configuration mode, display crypto accelerator statistics for specified protocols:

```
ciscoasa
 #
show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3

SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0

Failed requests: 0
ciscoasa
 #
show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
ciscoasa
 #
 show crypto protocol statistics ssl

[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
ciscoasa
 #
 show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
ciscoasa
 #
 show crypto protocol statistics all

[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
 SA creation requests: 1
   SA rekey requests: 3
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0

Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700

Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0

HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
ciscoasa #
```

Related Commands

Command	Description
clear crypto accelerator statistics	Clears the global and accelerator-specific statistics in the crypto accelerator MIB.
clear crypto protocol statistics	Clears the protocol-specific statistics in the crypto accelerator MIB.
show crypto accelerator statistics	Displays the global and accelerator-specific statistics from the crypto accelerator MIB.

show crypto sockets

To display crypto secure socket information, use the **show crypto sockets** command in global configuration mode or privileged EXEC mode.

show crypto sockets

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example, entered in global configuration mode, displays crypto secure socket information:

```
ciscoasa(config)# show crypto sockets
Number of Crypto Socket connections 1
       Gi0/1  Peers: (local): 2001:1::1
                     (remote): ::
              Local Ident (addr/plen/port/prot): (2001:1::1/64/0/89)
              Remote Ident (addr/plen/port/prot): (::/0/0/89)
              IPsec Profile: "CSSU-UTF"
              Socket State: Open
              Client: "CSSU_App(UTF)" (Client State: Active)
       Crypto Sockets in Listen state:
```

The following table describes the fields in the **show crypto sockets** command output.

Field	Description
Number of Crypto Socket connections	Number of crypto sockets in the system.

Field	Description
Socket State	This state can be Open, which means that active IPsec security associations (SAs) exist, or it can be Closed, which means that no active IPsec SAs exist.
Client	Application name and its state.
Flags	If this field says “shared,” the socket is shared with more than one tunnel interface.
Crypto Sockets in Listen state	Name of the crypto IPsec profile.

Related Commands

Command	Description
show crypto ipsec policy	Displays the crypto secure socket API installed policy information.

show csc node-count

To display the number of nodes for which the CSC SSM scanned traffic, use the **show csc node-count** command in privileged EXEC mode:

show csc node-count [**yesterday**]

Syntax Description

yesterday	(Optional) Shows the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight.

Command Default

By default, the node count displayed is the number of nodes scanned since midnight.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

A node is any distinct source IP address or the address of a device that is on a network protected by the ASA. The ASA keeps track of a daily node count and communicates this to the CSC SSM for user license enforcement.

Examples

The following is sample output of the **show csc node-count** command, which displays the number of nodes for which the CSC SSM has scanned traffic since midnight:

```
ciscoasa# show csc node-count
Current node count is 1
```

The following is sample output of the **show csc node-count** command, which displays the number of nodes for which the CSC SSM scanned traffic in the preceding 24-hour period, from midnight to midnight:

```
ciscoasa(config)# show csc node-count yesterday
Yesterday’s node count is 2
```

Related Commands

csc	Sends network traffic to the CSC SSM for scanning of FTP, HTTP, POP3, and SMTP, as configured on the CSC SSM.
show running-config class-map	Shows current class map configuration.
show running-config policy-map	Shows the current policy map configuration.

show running-config service-policy	Shows the current service policy configuration.

show ctiqbe

To display information about CTIQBE sessions established across the ASA, use the **show ctiqbe** command in privileged EXEC mode.

show ctiqbe

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show ctiqbe** command displays information of CTIQBE sessions established across the ASA. Along with **debug ctiqbe** and **show local-host**, this command is used for troubleshooting CTIQBE inspection engine issues.

Note We recommend that you have the **pager** command configured before using the **show ctiqbe** command. If there are a lot of CTIQBE sessions and the **pager** command is not configured, it can take a while for the **show ctiqbe** command output to reach the end.

Examples

The following is sample output from the **show ctiqbe** command under the following conditions. There is only one active CTIQBE session setup across the ASA. It is established between an internal CTI device (for example, a Cisco IP SoftPhone) at local address 10.0.0.99 and an external Cisco Call Manager at 172.29.1.77, where TCP port 2748 is the Cisco CallManager. The heartbeat interval for the session is 120 seconds.

```
ciscoasa# | show ctiqbe
Total: 1
        LOCAL           FOREIGN         STATE   HEARTBEAT
---------------------------------------------------------------
1       10.0.0.99/1117  172.29.1.77/2748        1       120
        ----------------------------------------------
```

```
RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 - 1029)
----------------------------------------------
MEDIA: Device ID 27     Call ID 0
       Foreign 172.29.1.99      (1028 - 1029)
       Local   172.29.1.88      (26822 - 26823)
----------------------------------------------
```

The CTI device has already registered with the CallManager. The device internal address and RTP listening port is PATed to 172.29.1.99 UDP port 1028. Its RTCP listening port is PATed to UDP 1029.

The line beginning with RTP/RTCP: PAT xlates: appears only if an internal CTI device has registered with an external CallManager and the CTI device address and ports are PATed to that external interface. This line does not appear if the CallManager is located on an internal interface, or if the internal CTI device address and ports are NATed to the same external interface that is used by the CallManager.

The output indicates a call has been established between this CTI device and another phone at 172.29.1.88. The RTP and RTCP listening ports of the other phone are UDP 26822 and 26823. The other phone locates on the same interface as the CallManager because the ASA does not maintain a CTIQBE session record associated with the second phone and CallManager. The active call leg on the CTI device side can be identified with Device ID 27 and Call ID 0.

Related Commands

Commands	Description
inspect ctiqbe	Enables CTIQBE application inspection.
service-policy	Applies a policy map to one or more interfaces.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show ctl-file

To show the contents of the CTL file used by the phone proxy, use the **show ctl-file** command in global configuration mode.

show ctl-file *filename* [**parsed**]

Syntax Description

filename	Displays the phones capable of secure mode stored in the database.
parsed	(Optional) Displays detailed information from the CTL file specified.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	The command was added.

Usage Guidelines

When specifying the filename of the CTL file stored in Flash memory, specify the disk number, filename, and extension; for example: disk0:/testctl.tlv . Using the **show ctl-file** command is useful for debugging when configuring the phone proxy instance.

Examples

The following example shows the use of the **show ctl-file** command to show general information about the CTL file:

```
ciscoasa# show ctl-file
disk0:/ctlfile.tlv

Total Number of Records: 1
CTL Record Number 1
  Subject Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Issuer Name:
     serialNumber=JMX1215L2TX+hostname=ciscoasa
  Function:
     cucm
  IP Address:
     192.168.52.102
  Associated Trustpoint:
     cucm_primary
```

```
The following example shows the use of the show ctl-file
command to show detailed information about the CTL file:
ciscoasa# show ctl-file
disk0:/ctlfile.tlv
 parsed
TAG 0x01: Version: Maj 1, Min 2
TAG 0x02: Header Len: Len 288
TAG 0x03: Signer ID: Len 103
TAG 0x04: Signer Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x05: Cert SN: Len 4 SN: c43c9048
TAG 0x06: CA Name: Len 45 Name: <cn=_internal_myctl_SAST_0,ou=STG,o=Cisco Inc>
TAG 0x07: Signature: Len 15
TAG 0x08: Digest Alg: Len 1 Name: SHA-1
TAG 0x09: Sig Alg Info: Len 8
TAG 0x0A: Sig Alg: Len 1 Name: RSA
TAG 0x0B: Modulus: Len 1 Name: 1024
TAG 0x0C: Sig Block: Len 128 Signature:
    521debcf b7a77ea8 94eba5f7 f3c8b0d8 3337a9fa 267ce1a7 202b2c8b 2ac980d3
    9608f64d e7cd82df e205e5bf 74a1d9c4 fae20f90 f3d2746a e90f439e ef93fca7
    d4925551 72daa414 2c55f249 ef7e6dc2 bcb9f9b5 39be8238 5011eecb ce37e4d1
    866e6550 6779c3fd 25c8bab0 6e9be32c 7f79fe34 5575e3af ea039145 45ce3158

TAG 0x0E: File Name: Len 12 Name: <CTLFile.tlv>
TAG 0x0F: Timestamp: Len 4 Timestamp: 48903cc6

 ### CTL RECORD No. 1 ###
TAG 0x01: Rcd Len: Len 731
TAG 0x03: Sub Name: Len 43 Sub Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x04: Function: Len 2 Func: CCM
TAG 0x05: Cert Issuer: Len 43 Issuer Name: <serialNumber=JMX1215L2TX+hostname=ciscoasa>
TAG 0x06: Cert SN: Len 4 Cert SN: 15379048
TAG 0x07: Pub Key: Len 140 Pub Key:
    30818902 818100ad a752b4e6 89769a49 13115e52 1209b3ef 96a179af 728c29d7
    af7fed4e c759d0ea cebd7587 dd4f7c4c 322da86b 3a677c08 ce39ce60 2525f6d2
    50fe87cf 2aea60a5 690ec985 10706e5a 30ad26db e6fdb243 159758ed bb487525
    f901ef4a 658445de 29981546 3867d2d1 ce519ee4 62c7be32 51037c3c 751c0ad6
    040bedbb 3e984502 03010001
TAG 0x09: Cert: Len 469 X.509v3 Cert:
    308201d1 3082013a a0030201 02020415 37904830 0d06092a 864886f7 0d010104
    0500302d 312b3012 06035504 05130b4a 4d583132 31354c32 54583015 06092a86
    4886f70d 01090216 08636973 636f6173 61301e17 0d303830 37333030 39343033
    375a170d 31383037 32383039 34303337 5a302d31 2b301206 03550405 130b4a4d
    58313231 354c3254 58301506 092a8648 86f70d01 09021608 63697363 6f617361
    30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00ada752
    b4e68976 9a491311 5e521209 b3ef96a1 79af728c 29d7af7f ed4ec759 d0eacebd
    7587dd4f 7c4c322d a86b3a67 7c08ce39 ce602525 f6d250fe 87cf2aea 60a5690e
    c9851070 6e5a30ad 26dbe6fd b2431597 58edbb48 7525f901 ef4a6584 45de2998
    15463867 d2d1ce51 9ee462c7 be325103 7c3c751c 0ad6040b edbb3e98 45020301
    0001300d 06092a86 4886f70d 01010405 00038181 005d82b7 ac45dbf8 bd911d4d
    a330454a a2784a4b 5ef898b1 482e0bbf 4a86ed86 9019820b 00e80361 fd7b2518
    9efa746c b98b1e23 fcc0793c de48de6d 6b1a4998 cd6f4e66 ba661d3a d200739a
    ae679c7c 94f550fb a6381b94 1eae389e a9ec4b11 30ba31f3 33cd184e 25647174
    ce00231d 102d5db3 c9c111a6 df37eb43 66f3d2d5 46
TAG 0x0A: IP Addr: Len 4 IP Addr: 192.168.52.102
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL instance to create for the phone proxy or parses the CTL file stored in Flash memory.
ctl-file (phone-proxy)	Specifies the CTL instance to use when configuring the phone proxy.

Command	Description
phone proxy	Configures the Phone Proxy instance.

show ctl-provider

To display the configuration of CTL providers used in unified communications, use the **show ctl-provider** command in privileged EXEC mode.

show ctl-provider [*name*]

Syntax Description

name	(Optional) Shows information for this CTL provider only.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

This example shows how to display the configuration of the CTL providers.

```
ciscoasa# show ctl-provider

!
ctl-provider my-ctl
 client interface inside address 192.168.1.55
 client interface inside address 192.168.1.56
 client username admin password gWe.oMSKmeGtelxS encrypted
 export certificate ccm-proxy
!
```

Related Commands

Command	Description
ctl-provider	Configures CTL providers.

show cts environment-data

To show the health and status of the environment data refresh operation on the ASA for Cisco TrustSec, use the **show cts environment-data** command in privileged EXEC mode.

show cts environment-data

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command is not supported on a standby device in a failover configuration. If you enter this command on a standby device, the following error message appears:

```
ERROR: This command is only permitted on the active device.
```

This command is only supported on the master unit in a clustering configuration. If you enter this command on a slave unit, the following error message appears:

```
This command is only permitted on the master device.
```

Examples

The following is sample output from the **show cts environment-data** command

```
ciscoasa# show cts environment-data
CTS Environment Data
====================
Status:                     Active
Last download attempt:      Successful
Environment Data Lifetime:  1200 secs
Last update time:           18:12:07 EST Feb 27 2012
Env-data expires in:        0:00:12:24 (dd:hr:mm:sec)
Env-data refreshes in:      0:00:02:24 (dd:hr:mm:sec)
```

Related Commands

Commands	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts pac	Shows the components on the PAC.

show cts environment-data sg-table

To show the resident security group table on the ASA for Cisco TrustSec, use the **show cts environment-data sg-table** command in privileged EXEC mode.

show cts environment-data sg-table

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command is not supported on a standby device in a failover configuration. If you enter this command on a standby device, the following error message appears:

```
ERROR: This command is only permitted on the active device.
```

This command is only supported on the master unit in a clustering configuration. If you enter this command on a slave unit, the following error message appears:

```
This command is only permitted on the master device.
```

Examples

The following is sample output from the **show cts environment-data sg-table** command

```
ciscoasa# show cts environment-data sg-table
Security Group Table:
Valid until: 18:32:07 EST Feb 27 2012
Showing 9 of 9 entries
SG Name                          SG Tag     Type
-------                          ------     -------------
ANY                               65535     unicast
ExampleSG1                            2     unicast
ExampleSG13                          14     unicast
ExampleSG14                          15     unicast
ExampleSG15                          16     unicast
ExampleSG16                          17     unicast
```

```
ExampleSG17                           18     unicast
ExampleSG18                           19     unicast
Unknown                                0     unicast
```

Related Commands

Commands	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts pac	Shows the components on the PAC.

show cts pac

To show the components of the Protected Access Credential (PAC) on the ASA for Cisco TrustSec, use the **show cts pac** command in privileged EXEC mode.

show cts pac

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show cts pac** command displays PAC information, including the expiration time. The expiration time is important because the ASA cannot retrieve security group table updates after the PAC lifetime lapses. The administrator must request and install a new PAC before the old one expires to maintain synchronization with the security group table on the Identity Services Engine.

This command is not supported on a standby device in a failover configuration. If you enter this command on a standby device, the following error message appears:

```
ERROR: This command is only permitted on the active device.
```

This command is only supported on the master unit in a clustering configuration. If you enter this command on a slave unit, the following error message appears:

```
This command is only permitted on the master device.
```

Examples

The following is sample output from the **show cts pac** command

```
ciscoasa# show cts pac
PAC-Info:
    Valid until: Jul 28 2012 08:03:23
    AID:         6499578bc0240a3d8bd6591127ab270c
    I-ID:        BrianASA36
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
```

```
PAC-Opaque:
  000200b000030001000400106499578bc0240a3d8bd6591127ab270c00060094000301
  00d75a3f2293ff3b1310803b9967540ff7000000134e2d2deb00093a803d227383e2b9
  7db59ed2eeac4e469fcb1eeb0ac2dd84e76e13342a4c2f1081c06d493e192616d43611
  8ff93d2af9b9135bb95127e8b9989db36cf1667b4fe6c284e220c11e1f7dbab91721d1
  00e9f47231078288dab83a342ce176ed2410f1249780882a147cc087942f52238fc9b4
  09100e1758
```

Related Commands

Commands	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show cts sgt-map

To show the IP address-security group table manager entries in the control path, use the **show cts sgt-map** command in privileged EXEC mode.

show cts sgt-map [**sgt** *sgt*] [**address** *ip4* [/ *mask*] | **address** *ipv6* [/ *prefix*] **| ipv4 | ipv6**] [**name**] [**brief | detail**]

Syntax Description

address {*ipv4* [/*mask*] /*ipv6* [/*prefix*]}	Shows only IP address-security group table mapping for the specific IPv4 or IPv6 address. Include an IPv4 subnet mask or IPv6 prefix to see the mapping for a network.
brief	Shows the IP address-security group table mapping summary.
detail	Shows the IP address-security group table mapping.
ipv4	Shows the IPv4 address-security group table mapping. By default, only the IPv4 address-security group table mapping is displayed.
ipv6	Shows the IPv6 address-security group table mapping.
name	Shows IP address-security group table mapping with the matched security group name.
sgt *sgt*	Shows only IP address-security group table mapping with the matched security group table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.01)	The command was added.
9.3(1)	The output was updated to include IP-SGT binding information from the "CLI-HI" source, which is populated by the **cts role-based sgt-map** command.
9.6(1)	The ability to show network mappings was added.

Usage Guidelines

This command displays the IP address-security group table manager entries in the control path.

Examples

The following is sample output from the **show cts sgt-map** command:

```
ciscoasa# show cts sgt-map
Active IP-SGT Bindings Information
IP Address    SGT Source
============================================
1.1.1.1       7 CLI-HI
10.10.10.1    7 CLI-HI
10.10.10.10   3 LOCAL
10.10.100.1   7 CLI-HI
198.26.208.31 7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

The following is sample output from the **show cts sgt-map** command with some network bindings.

```
ciscoasa# show cts sgt-map

Active IP-SGT Bindings Information
IP Address       SGT Source
============================================
10.1.1.1          7   CLI-HI
10.252.10.0/24   7   CLI-HI
10.252.10.10     3   LOCAL
10.252.100.1     7   CLI-HI
172.26.0.0/16    7   SXP
IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of CLI-HI   bindings = 3
Total number of SXP      bindings = 1
Total number of active   bindings = 5
```

The following is sample output from the **show cts sgt-map ipv6** command:

```
ciscoasa# show cts sgt-map ipv6
Active IP-SGT Bindings Information
IP Address                              SGT     Source
============================================================
3330::1                                 17      SXP
FE80::A8BB:CCFF:FE00:110                17      SXP
IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 2
Total number of active   bindings = 2
```

The following is sample output from the **show cts sgt-map ipv6 detail** command:

```
ciscoasa# show cts sgt-map ipv6 detail
Active IP-SGT Bindings Information
IP Address                 Security Group                         Source
=========================================================================
3330::1                     2345                                    SXP
1280::A8BB:CCFF:FE00:110    Security Tech Business Unit(12345)      SXP
IP-SGT Active Bindings Summary
```

```
===================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

The following is sample output from the **show cts sgt-map ipv6 brief** command:

```
ciscoasa# show cts sgt-map ipv6 brief
Active IP-SGT Bindings Information
IP-SGT Active Bindings Summary
====================================
Total number of SXP bindings    = 2
Total number of active bindings = 2
```

The following is sample output from the **show cts sgt-map address** command:

```
ciscoasa# show cts sgt-map address 10.10.10.5
Active IP-SGT Bindings Information
IP Address              SGT     Source
============================================================
10.10.10.5              1234    SXP
IP-SGT Active Bindings Summary
============================================
Total number of SXP    bindings = 1
Total number of active   bindings = 1
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show cts sxp connections

To show the Security eXchange Protocol (SXP) connections on the ASA, use the **show cts sxp connections** command in privileged EXEC mode.

show cts sxp connections [**peer** *peer addr*] [**local** *local addr*] [**ipv4 | ipv6**] [**status** { **on | off | delete-hold-down | pending-on** }] [**mode** { **speaker | listener** }] [**brief**]

Syntax Description

brief	(Optional) Shows the SXP connection summary.
delete-hold-down	(Optional) The TCP connection was terminated (TCP is down) when it was in the ON state. Only an ASA configured in listener mode can be in this state.
ipv4	(Optional) Shows SXP connections with IPv4 addresses.
ipv6	(Optional) Shows SXP connections with IPv6 addresses.
listener	(Optional) Shows the ASA configured in listener mode.
local *local addr*	(Optional) Shows SXP connections with the matched local IP addresses.
mode	(Optional) Shows SXP connections with the matched mode.
off	(Optional) The TCP connection has not been initiated. The ASA retries the TCP connection only in this state.
on	(Optional) An SXP OPEN or SXP OPEN RESP message has been received. The SXP connection has been successfully established. The ASA only exchanges SXP messages in this state.
peer *peer addr*	(Optional) Shows SXP connections with the matched peer IP addresses.
pending-on	(Optional) An SXP OPEN message has been sent to the peer; the response from the peer is being awaited.
speaker	(Optional) Shows the ASA configured in speaker mode.
status	(Optional) Shows SXP connections with the matched status.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	The command was added.

Usage Guidelines

The SXP states change under the following conditions:

- If the SXP listener drops its SXP connection because its peer unconfigures SXP or disables SXP, then the SXP listener moves to the OFF state.
- If the SXP listener drops its SXP connection because its peer crashes or has the interface shut down, then the SXP listener moves to the DELETE_HOLD_DOWN state.
- The SXP speaker moves to the OFF state when either of the first two conditions occurs.

This command is supported on the active device only in failover mode, and the master unit only in a cluster.

Examples

The following is sample output from the **show cts sxp connections** command:

```
ciscoasa# show cts sxp connections
SXP                : Enabled
Highest version    : 2
Default password   : Set
Default local IP   : Not Set
Delete hold down period : 120 secs
Reconcile period   : 120 secs
Retry open period : 10 secs
Retry open timer   : Not Running
Total number of SXP connections : 3
Total number of SXP connection shown : 3
----------------------------------------------
Peer IP            : 2.2.2.1
Local IP           : 2.2.2.2
Conn status        : On
Local mode         : Listener
Ins number         : 1
TCP conn password : Default
Delete hold down timer : Not Running
Reconciliation timer    : Not Running
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 3.3.3.1
Local IP           : 3.3.3.2
Conn status        : On
Local mode         : Listener
Ins number         : 2
TCP conn password : None
Delete hold down timer : Not Running
Reconciliation timer    : Not Running
Duration since last state change: 0:01:02:20 (dd:hr:mm:sec)
----------------------------------------------
Peer IP            : 4.4.4.1
Local IP           : 4.4.4.2
Conn status        : On
Local mode         : Speaker
Ins number         : 1
TCP conn password : Set
Delete hold down timer : Not Running
Reconciliation timer    : Not Running
Duration since last state change: 0:03:01:20 (dd:hr:mm:sec)
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show cts sxp sgt-map

To show the current IP address-security group table mapping database entries in the Security eXchange Protocol (SXP) module on the ASA for Cisco TrustSec, use the **show cts sxp sgt-map** command in privileged EXEC mode.

show cts sxp sgt-map [**peer** *peer_addr*] [**sgt** *sgt*] [**address** *ipv4* [/ *mask*] | **address** *ipv6* [/ *prefix*] | **ipv4** | **ipv6**] [**name**] [**brief** | **detail**] [**status**]

Syntax Description

address {*ipv4* [/*mask*] /*ipv6* [/*prefix*]}	Shows only IP address-security group table mapping for the specific IPv4 or IPv6 address. Include an IPv4 subnet mask or IPv6 prefix to see the mapping for a network.
brief	Shows the IP address-security group table mapping summary.
detail	Shows the security group table information. If a security group name is not available, only the security group table value is displayed without the bracket.
ipv4	Shows the IP address-security group table mapping with IPv4 addresses. By default, only the IP address-security group table mapping with IPv4 addresses is displayed.
ipv6	Shows the IP address-security group table mapping with IPv6 addresses.
name	Shows IP address-security group table mapping with the matched security group name.
peer *peer addr*	Shows only IP address-security group table mapping with the matched peer IP address.
sgt *sgt*	Shows only IP address-security group table mapping with the matched security group table.
status	Shows active or inactive mapped entries.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.01)	The command was added.
9.6(1)	The ability to show network mappings was added.

Usage Guidelines

This command displays the active IP address-security group table mapped entries consolidated from SXP.

This command is not supported on a standby device in a failover configuration. In a cluster, enter the command on the master unit.

Examples

The following is sample output from the **show cts sxp sgt-map** command:

```
ciscoasa# show cts sxp sgt-map
Total number of IP-SGT mappings : 3
SGT         : 7
IPv4        : 2.2.2.1
Peer IP     : 2.2.2.1
Ins Num     : 1
SGT         : 7
IPv4        : 2.2.2.0
Peer IP     : 3.3.3.1
Ins Num     : 1
SGT         : 7
IPv6        : FE80::A8BB:CCFF:FE00:110
Peer IP     : 2.2.2.1
Ins Num     : 1
```

The following is sample output from the **show cts sxp sgt-map detail** command:

```
ciscoasa# show cts sxp sgt-map detail
Total number of IP-SGT mappings : 3
SGT         : STBU(7)
IPv4        : 2.2.2.1
Peer IP     : 2.2.2.1
Ins Num     : 1
Status      : Active
SGT         : STBU(7)
IPv4        : 2.2.2.0
Peer IP     : 3.3.3.1
Ins Num     : 1
Status      : Inactive
SGT         : 6
IPv6        : 1234::A8BB:CCFF:FE00:110
Peer IP     : 2.2.2.1
Ins Num     : 1
Status      : Active
```

The following is sample output from the **show cts sxp sgt-map brief** command. Some mappings are to networks.

```
ciscoasa# show cts sxp sgt-map brief
Total number of IP-SGT mappings : 3
SGT, IPv4: 7, 2.2.2.0/24
SGT, IPv4: 7, 3.3.3.3
SGT, IPv6: 7, FE80::0/64
```

Related Commands

Command	Description
show running-config cts	Shows the SXP connections for the running configuration.
show cts environment	Shows the health and status of the environment data refresh operation.

show curpriv

To display the current user privileges, use the **show curpriv** command:

show curpriv

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes
Privileged EXEC	• Yes	• Yes	—	—	• Yes
User EXEC	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	Modified to conform to CLI guidelines.

Usage Guidelines

The **show curpriv** command displays the current privilege level. Lower privilege level numbers indicate lower privilege levels.

Examples

These examples show output from the **show curpriv** command when a user named enable_15 is at different privilege levels. The username indicates the name that the user entered when the user logged in. P_PRIV indicates that the user has entered the **enable** command. P_CONF indicates that the user has entered the **config terminal** command.

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa(config)# exit
ciscoasa(config)# show curpriv
Username : enable_1
```

```
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa(config)#
```

The following example shows a known behavior. When you are in enable mode, then enter disable mode, the initial logged-in username is replaced with enable_1:

```
ciscoasa(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
ciscoasa(config)# exit
ciscoasa# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
ciscoasa# exit
Logoff
Type help or '?' for a list of available commands.
ciscoasa# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
ciscoasa#
```

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
show running-config privilege	Display privilege levels for commands.

show d – show e

show data-plane quick-reload status

To view the state of the data plane reload, use the **show data-plane quick-reload status** command in privileged EXEC mode.

show data-plane quick-reload status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global Configuration Mode	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.20(2)	This command was added.

Usage Guidelines

This command displays the quick reload status of the data path for the current context.

Examples

The following is sample output for the **show data-plane quick-reload status** command when the data plane quick reload is enabled:

```
ciscoasa# show data-plane quick-reload status
data-plane reloaded!
```

The following is sample output for the **show data-plane quick-reload status** command when the data plane quick reload is disabled:

```
ciscoasa# show data-plane quick-reload status
device reloaded
```

Related Commands

Command	Description
data-plane quick-reload	Enables data-plane quick-reload.

show ddns update interface

To display the DDNS methods assigned to ASA interfaces, use the **show ddns update interface** command in privileged EXEC mode.

show ddns update interface [*interface-name*]

Syntax Description

interface-name	(Optional) The name of a network interface.

Command Default

Omitting the *interface-name* string displays the DDNS method assigned to each interface.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.15(1)	For the Web update method, the output of this command includes the last successful updated FQDN/IP address mapping.

Examples

The following example displays the DDNS method assigned to the inside interface:

```
ciscoasa# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
ciscoasa#
```

The following example shows a successful web type update:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

The following example shows a web type failure:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

The following example shows that the DNS server returned an error for the web type update:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

The following example shows that a web update was not yet attempted due to the IP address unconfigured or the DHCP request failed, for example:

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

Related Commands

Command	Description
ddns	Specifies the standard DDNS update method type.
ddns update	Associates a DDNS method with an interface.
ddns update method	Creates a DDNS update method.
interval maximum	Configures the update interface between DNS requests.
show ddns update method	Displays the type and interval for each configured DDNS method. a DHCP server to perform DDNS updates.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.
web update-type	Specifies the address types (IPv4 or IPv6) that you want to update.
web update-url	Sets the DDNS update method to Web and sets the update URL.

show ddns update method

To display the DDNS update methods in the running configuration, use the **show ddns update method** command in privileged EXEC mode.

show ddns update method [*method-name*]

Syntax Description

method-name	(Optional) The name of a configured DDNS update method.

Command Default

Omitting the *method-name* string displays all configured DDNS update methods.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
9.15(1)	Output for the Web update method was added.
9.18(1)	Output for the Web update method was enhanced to display the configured reference-identity.

Examples

The following example displays the DDNS method named ddns-2:

```
ciscoasa(config)# show ddns update method ddns-2
 Dynamic DNS Update Method: ddns-2
 IETF standardized Dynamic DNS 'A' and 'PTR' records update
 Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
 ciscoasa(config)#
```

The following example shows details about the web update method:

```
 ciscoasa# show ddns update method web1
Dynamic DNS Update Method: web1
Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
pwd@10.x.x.x/update?hostname=<>https://admin:pwd@10.x.x.x/update?hostname=<;h>&myip=<a>
  Update type configured: ipv4
  Configured reference-identity name: dyndns
  Maximum update interval: 0 days 0 hours 2 minutes 0 seconds
```

Related Commands

Command	Description
ddns	Specifies a DDNS update method type for a created DDNS method.
ddns update	Associates a ASA interface with a Dynamic DNS (DDNS) update method or a DDNS update hostname.
ddns update method	Creates a method for dynamically updating DNS resource records.
show ddns update interface	Displays the interfaces associated with each configured DDNS method.
show running-config ddns	Displays the type and interval of all configured DDNS methods in the running configuration.

show debug

To show the current debugging configuration, use the **show debug** command.

show debug [*command* [*keywords*]]

Syntax Description

command	(Optional) Specifies the **debug** command whose current configuration you want to view.
keywords	(Optional) For each *command* , the *keywords* following the *command* are identical to the *keywords* supported by the associated **debug** command.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **eigrp** keyword was added to the list of possible command values.
8.4(1)	The **route** keyword was added to the list of possible command values.
9.2(1)	The **event manager** keyword was added to the list of possible command values.
9.5(2)	The output has been modified to include any debug persistent settings.
9.5(2)	The ability to show debug logs by filtering, based on the filter condition sets was added.

Usage Guidelines

For each *command* , the *keywords* following the *command* are identical to the *keywords* supported by the associated **debug** command. For information about the supported syntax, see the associated **debug** command.

Note The availability of each *command* depends on the command modes that support the applicable **debug** command.

The valid *command* values are as follows:

- **aaa**

- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **cxsc**
- **debug eigrp parser**
- **dhcpc**
- **dhcpd**
- **dhcprelay**
- **disk**
- **dns**
- **eigrp**
- **email**
- **entity**
- event manager
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ipv6 eigrp**
- **ipv6 eigrp neighbor**
- **ipv6 eigrp notifications**

- **ipv6 eigrp summary**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mmp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **route**
- **rtsp**
- **sdi**
- **sequence**
- **sfr**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**
- **ssl**

- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**
- **xml**

Examples

You can use the **show debug** command to view all debugging configurations, a debugging configuration for a specific feature, and a debugging configuration for a portion of a feature.

The following commands enable debugging for authentication, accounting, and flash memory:

```
ciscoasa# debug aaa authentication

debug aaa authentication enabled at level 1
ciscoasa# debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa# debug disk filesystem
debug disk filesystem enabled at level 1
ciscoasa# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
ciscoasa# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
ciscoasa# show debug aaa accounting
debug aaa accounting enabled at level 1
ciscoasa#
```

Related Commands

Command	Description
debug	Displays all **debug** commands.

show dhcpd

To view DHCP binding, state, and statistical information, use the **show dhcpd** command in privileged EXEC or global configuration mode.

show dhcpd { **binding** [*IP_address*] **| state | statistics** }

Syntax Description

binding	Displays binding information for a given server IP address and its associated client hardware address and lease length.
IP_address	Shows the binding information for the specified IP address.
state	Displays the state of the DHCP server, such as whether it is enabled in the current context and whether it is enabled on each of the interfaces.
statistics	Displays statistical information, such as the number of address pools, bindings, expired bindings, malformed messages, sent messages, and received messages.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you include the optional IP address in the **show dhcpd binding** command, only the binding for that IP address is shown.

The **show dhcpd binding | state | statistics** commands are also available in global configuration mode.

Examples

The following is sample output from the **show dhcpd binding** command:

```
ciscoasa# show dhcpd binding
IP Address Client-id        Lease  Expiration  Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

The following is sample output from the **show dhcpd state** command:

```
ciscoasa# show dhcpd state
```

```
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

The following is sample output from the **show dhcpd statistics** command:

```
ciscoasa# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0
Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
clear dhcpd	Clears the DHCP server bindings and statistic counters.
dhcpd lease	Defines the lease length for DHCP information granted to clients.
show running-config dhcpd	Displays the current DHCP server configuration.

show dhcprelay state

To view the state of the DHCP relay agent, use the **show dhcprelay state** command in privileged EXEC or global configuration mode.

show dhcprelay state

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays the DHCP relay agent state information for the current context and each interface.

Examples

The following is sample output from the **show dhcprelay state** command:

```
ciscoasa# show dhcprelay state
Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

Related Commands

Command	Description
show dhcpd	Displays DHCP server statistics and state information.
show dhcprelay statistics	Displays the DHCP relay statistics.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show dhcprelay statistics

To display the DHCP relay statistics, use the **show dhcprelay statistics** command in privileged EXEC mode.

show dhcprelay statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The output of the **show dhcprelay statistics** command increments until you enter the **clear dhcprelay statistics** command.

Examples

The following shows sample output for the **show dhcprelay statistics** command:

```
ciscoasa# show dhcprelay statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0
Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
ciscoasa#
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.

Command	Description
clear dhcprelay statistics	Clears the DHCP relay agent statistic counters.
debug dhcprelay	Displays debug information for the DHCP relay agent.
show dhcprelay state	Displays the state of the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

show diameter

To display state information for each Diameter connection, use the **show diameter** command in privileged EXEC mode.

show diameter

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

To display Diameter connection state information, you must inspect Diameter traffic.

Examples

The following shows sample output for the **show diameter** command:

```
ciscoasa# show diameter

Total active diameter sessions: 5
Session 3638
        ==========
        ref_count: 1 val = .; 1096298391; 2461;
            Protocol : diameter Context id : 0
            From inside:211.1.1.10/45169 to outside:212.1.1.10/3868
...
```

Related Commands

Command	Description
clear service-policy	Clears service policy statistic.
inspect diameter	Inspects Diameter traffic.

show disk

To display the contents of the flash memory for the ASA only, use the **show disk** command in privileged EXEC mode.

show disk [**0 | 1**] [**filesys | all**] **controller**

Syntax Description

0 | 1	Specifies the internal flash memory (0, the default) or the external flash memory (1).
all	Shows the contents of flash memory plus the file system information.
controller	Specifies the flash controller model number.
filesys	Shows information about the compact flash card.

Command Default

By default, this command shows the internal flash memory.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show disk** command:

```
ciscoasa# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log
10170368 bytes available (52711424 bytes used)
```

The following is sample output from the **show disk filesys** command:

```
ciscoasa# show disk filesys
******** Flash Card Geometry/Format Info ********
COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184
COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

The following is sample output from the **show disk controller** command:

```
ciscoasa# show disk:1 controller
Flash Model: TOSHIBA THNCF064MBA
```

Related Commands

Command	Description
dir	Displays the directory contents.

show dns

To show the current resolved DNS addresses for fully qualified domain name (FQDN) hosts, and the trusted DNS source configuration, use the **show dns** command in privileged EXEC mode.

show dns [**host** *fqdn_name* | **ip-cache** [**count**] | **trusted-source** [**detail**]]

Syntax Description

host*fqdn_name*	(Optional) Limits the command to show information about the specified fully-qualified domain name (FQDN) only.
ip-cache [**count**]	(Optional.) Show the contents of the IP cache created by snooping DNS responses for network-service object domain specifications. Include the **count** keyword if you only want to see the number of items in the cache.
trusted-source [**detail**]	(Optional.) Show the configuration for trusted DNS servers, which are snooped for network-service object domain resolution. Include the **detail** keyword to show the IP addresses of all trusted DNS servers.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.17(1)	Without parameters, the **show dns** command and **show dns-hosts** commands provide the same information. We also added the **ip-cache** and **trusted-source** keywords.

Examples

The following is sample output from the **show dns** command. If no FQDN host has not been activated yet, this command shows no output.

```
ciscoasa# show dns
Name:   www.example1.com
  Address: 10.1.3.1                             TTL 00:03:01
  Address: 10.1.3.3                             TTL 00:00:36
  Address: 10.4.1.2                             TTL 00:01:01
Name: www.example2.com
  Address: 10.2.4.1                             TTL 00:25:13
  Address: 10.5.2.1                             TTL 00:25:01
```

```
Name: server.ddns-exampleuser.com
  Address: fe80::21e:8cff:feb5:4faa             TTL 00:00:41
  Address: 10.10.10.2                           TTL 00:25:01
```

The following is sample output from the **show dns host** command:

```
ciscoasa# show dns host www.example.com
Name:   www.example.com
Address: 10.1.3.1 TTL 00:03:01
Address: 10.1.9.5 TTL 00:00:36
Address: 10.1.1.2 TTL 00:01:01
```

Starting with 9.17(1), the command without parameters shows the same information as the **show dns-hosts** command, and includes information on the trusted DNS sources used for network-service object domain resolution, and the IP cache.

```
ciscoasa# show dns
Host                     Flags      Age Type   Address(es)
sngdc01-ucs-dcz01n-gslb1-(temp, OK) 0    IP    173.39.112.230
alln01-ucs-dcz03n-gslb1-s(temp, OK) 0    IP    173.37.151.38
rcdn9-ucs-dcz05n-gslb1-sn(temp, OK) 0    IP    72.163.7.198
aer01-ucs-dcz01n-gslb1-sn(temp, OK) 0    IP    173.38.213.70
rtp5-ucs-dcz01n-gslb1-sni(temp, OK) 0    IP    64.101.37.118
mtv5-ucs-dcz06n-gslb1-sni(temp, OK) 0    IP    173.36.225.38
www.cisco.com            (temp, OK) 0    IP    72.163.4.161
       origin-www.cisco.com
DNS Trusted Source enabled for DHCP Server Configured
DNS Trusted Source enabled for DHCP Client Learned
DNS Trusted Source enabled for DHCP Relay Learned
DNS Trusted Source enabled for DNS Server Configured
DNS Trusted Source not enabled for Trust-any
DNS Trusted Source: Type: IPs : Interface : Idle/Timeout (sec)
    DNS Server Configured: 72.163.47.11: management : N/A
    DNS Server Configured: 173.37.137.85: management : N/A
    DNS Server Configured: 173.37.142.73: management : N/A
DNS snooping IP cache: 0 in use, 0 most used
Address                              Idle(sec) Timeout(sec) Hit-count          Branch(es)
```

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
clear ip-cache	Clears the cache built by snooping DNS responses for network-service object domain specifications.
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
dns trusted-source	Identifies the trusted DNS servers.

show dns-hosts

To show the DNS cache, use the **show dns-hosts** command in privileged EXEC mode. The DNS cache includes dynamically learned entries from a DNS server and manually entered names and IP addresses.

show dns-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show dns-hosts** command:

```
ciscoasa# show dns-hosts
Host                           Flags      Age Type   Address(es)
ns2.example.com                (temp, OK) 0    IP    10.102.255.44
ns1.example.com                (temp, OK) 0    IP    192.168.241.185
snowmass.example.com           (temp, OK) 0    IP    10.94.146.101
server.example.com             (temp, OK) 0    IP    10.94.146.80
```

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.

Table 11 shows each field description.

Table 42: show dns-hosts Fields

Field	Description
Host	Shows the hostname.
Flags	Shows the entry status as a combination of the following: • temp—This entry is temporary because it comes from a DNS server. The ASA removes this entry after 72 hours of inactivity. • perm—This entry is permanent because it was added with the name command. • OK—This entry is valid. • ??—This entry is suspect and needs to be revalidated. • EX—This entry is expired.
Age	Shows the number of hours since this entry was last referenced.
Type	Shows the type of DNS record; this value is always IP.
Address(es)	The IP addresses.

Related Commands

Command	Description
clear dns-hosts	Clears the DNS cache.
dns domain-lookup	Enables the ASA to perform a name lookup.
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the ASA does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.

show dynamic-filter data

To show information about the Botnet Traffic Filter dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries, use the **show dynamic-filter data** command in privileged EXEC mode.

show dynamic-filter data

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

To view dynamic database information, first enable use and download of the database with the **dynamic-filter use-database** and **dynamic-filter updater-client enable** commands.

Examples

The following is sample output from the **show dynamic-filter data** command:

```
ciscoasa# show dynamic-filter data
Traffic filter is using downloaded database version '907'
Fetched at 18:00:16 UTC Jan 22 2009, size: 674381
Sample names from downloaded database:
  example.com, example.net, example.org,
cisco.example, cisco.invalid, bad.example.com
bad.example.net, bad.example.org, bad.cisco.example
bad.cisco.ivalid
Total entries in Dynamic Filter database:
  Dynamic data: 40909 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
Active rules in Dynamic Filter asp table:
  Dynamic data: 0 domain names , 1080 IPv4 addresses
  Local data: 0 domain names , 0 IPv4 addresses
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show dynamic-filter dns-snoop

To show the Botnet Traffic Filter DNS snooping summary, or the actual IP addresses and names, use the **show dynamic-filter dns-snoop** command in privileged EXEC mode.

show dynamic-filter dns-snoop [**detail**]

Syntax Description

detail	(Optional) Shows the IP addresses and names snooped from DNS responses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Usage Guidelines

All inspected DNS data is included in this output, and not just matching names in the blacklist. DNS data from static entries are not included.

To clear the DNS snooping data, enter the **clear dynamic-filter dns-snoop** command.

Examples

The following is sample output from the **show dynamic-filter dns-snoop** command:

```
ciscoasa# show dynamic-filter dns-snoop
DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
```

The following is sample output from the **show dynamic-filter dns-snoop detail** command:

```
ciscoasa# show dynamic-filter dns-snoop detail
DNS Reverse Cache Summary Information:
75 addresses, 124 names, 997 dnsrc address buckets
DNS reverse Cache Information:
[10.67.22.34] flags=0x22, cat=2, unit=0 b:g:w=3:0:0, cookie=0xda148218
    [www3.example.com] cat=2, ttl=3
    [www.bad.example.com] cat=2, ttl=3
    [www.example.com] cat=2, ttl=3
[10.6.68.133] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda13ed60
    [cisco.example] cat=2, ttl=73
```

```
[10.166.226.25] flags=0x2, cat=2, unit=0 b:g:w=1:0:0, cookie=0xda608cb8
    [cisco.invalid] cat=2, ttl=2
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter reports	Generates reports of the top 10 botnet sites, ports, and infected hosts.

Command	Description
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show dynamic-filter reports infected-hosts

To generate reports about infected hosts classified by the Botnet Traffic Filter, use the **show dynamic-filter reports infected-hosts** command in privileged EXEC mode.

show dynamic-filter reports infected-hosts [**max-connections | latest-active | highest-threat |subnet** *ip_address netmask* | **all**]

Syntax Description

all	Shows all buffered infected-hosts information. This display might include thousands of entries. You might want to use ASDM to generate a PDF file instead of using the CLI.
highest-threat	Shows the 20 hosts that connected to the malware sites with the highest threat level.
latest-active	Shows the 20 hosts with the most recent activity. For each host, the display shows detailed information about 5 visited malware sites.
max-connections	Shows the 20 infected hosts with the most number of connections.
subnet *ip_address netmask*	Shows up to 20 hosts within the specified subnet.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(2)	This command was added.

Usage Guidelines

These reports contain detailed history about infected hosts, showing the correlation between infected hosts, visited malware sites, and malware ports.

To clear the report data, enter the **clear dynamic-filter reports infected-hosts** command.

Examples

The following is sample output from the **show dynamic-filter reports infected hosts all** command:

```
ciscoasa#
                  show
```

dynamic-filter reports infected-hosts all

```
Total 2 infected-hosts in buffer

Host (interface)                        Latest malicious conn time, filter action  Conn
logged, dropped

=========================================================================================

192.168.1.4 (internal)                  15:39:40 UTC Sep 17 2009, dropped
   3      3

Malware-sites connected to (not ordered)

Site                       Latest conn port, time, filter action   Conn logged, dropped
Threat-level Category

-----------------------------------------------------------------------------------------

10.73.210.27 (bad.example.com)     80, 15:39:31 UTC Sep 17 2009, dropped      2   2
very-high Malware

10.65.2.119 (bad2.example.com)     0, 15:39:40 UTC Sep 17 2009, dropped       1   1
very-high admin-added

=========================================================================================

192.168.1.2 (internal)                  15:39:01 UTC Sep 17 2009, dropped
   5      5

Malware-sites connected to (not ordered)

Site                       Latest conn port, time, filter action   Conn logged, dropped
Threat-level Category

-----------------------------------------------------------------------------------------

10.131.36.158 (bad.example.com)    0, 15:37:46 UTC Sep 17 2009, dropped      1    1
very-high admin-added

10.65.2.119 (bad2.example.com)     0, 15:37:53 UTC Sep 17 2009, dropped      1    1
very-high  admin-added

20.73.210.27 (bad3.example.com)   80, 15:39:01 UTC Sep 17 2009, dropped      3    3
very-high  Malware

=========================================================================================


Last clearing of the infected-hosts report: Never
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.

Command	Description
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show dynamic-filter reports top

To generate reports of the top 10 malware sites, ports, and infected hosts classified by the Botnet Traffic Filter, use the **show dynamic-filter reports top** command in privileged EXEC mode.

show dynamic-filter reports top [**malware-sites** | **malware-ports** | **infected-hosts**]

Syntax Description

malware-ports	(Optional) Shows a report for the top 10 malware ports.
malware-sites	(Optional) Shows a report for the top 10 malware sites.
infected-hosts	(Optional) Shows a report for the top 10 infected hosts.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
8.2(2)	The **botnet-sites** and **botnet-ports** keywords were changed to **malware-sites** and **malware-ports**. The malware-sites report now includes the number of connections dropped, and the threat level and category of each site. A last clear timestamp was added. For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

This report is a snapshot of the data, and may not match the top 10 items since the statistics started to be collected.

To clear the report data, enter the **clear dynamic-filter reports top** command.

Examples

The following is sample output from the **show dynamic-filter reports top malware-sites** command:

```
ciscoasa# show dynamic-filter reports top malware-sites
Site                             Connections logged dropped Threat Level Category
--------------------------------------------------------------------------------------
bad1.example.com (10.67.22.34)                11      0          2      Botnet
bad2.example.com (209.165.200.225)             8      8          3      Virus
bad1.cisco.example(10.131.36.158)              6      6          3      Virus
bad2.cisco.example(209.165.201.1)              2      2          3      Trojan
```

```
horrible.example.net(10.232.224.2)                   2     2          3      Botnet
nono.example.org(209.165.202.130)                    1     1          3      Virus
Last clearing of the top sites report: at 13:41:06 UTC Jul 15 2009
```

The following is sample output from the **show dynamic-filter reports top malware-ports** command:

```
ciscoasa# show dynamic-filter reports top malware-ports
Port                                       Connections logged
----------------------------------------------------------------------
tcp 1000                                           617
tcp 2001                                           472
tcp 23                                              22
tcp 1001                                            19
udp 2000                                            17
udp 2001                                            17
tcp 8080                                             9
tcp 80                                               3
tcp >8192                                            2
Last clearing of the top ports report: at 13:41:06 UTC Jul 15 2009
```

The following is sample output from the **show dynamic-filter reports top infected-hosts** command:

```
ciscoasa# show dynamic-filter reports top infected-hosts
Host                                       Connections logged
----------------------------------------------------------------------
10.10.10.51(inside)                               1190
10.12.10.10(inside)                                10
10.10.11.10(inside)                                 5
Last clearing of the top infected-hosts report: at 13:41:06 UTC Jul 15 2009
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.

Command	Description
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show dynamic-filter statistics

To show how many connections were classified as whitelist, blacklist, and greylist connections using the Botnet Traffic Filter, use the **show dynamic-filter statistics** command in privileged EXEC mode.

show dynamic-filter statistics [**interface** *name*] [**detail**]

Syntax Description

detail	(Optional) Shows how many packets at each threat level were classified or dropped.
interface *name*	(Optional) Shows statistics for a particular interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
8.2(2)	The **detail** keyword was added to show how many packets at each threat level were classified or dropped. For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The greylist includes addresses that are associated with multiple domain names, but not all of these domain names are on the blacklist.

To clear the statistics, enter the **clear dynamic-filter statistics** command.

Examples

The following is sample output from the **show dynamic-filter statistics** command:

```
ciscoasa# show dynamic-filter statistics
Enabled on interface outside
 Total conns classified 11, ingress 11, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 11, dropped 5, ingress 11, egress 0
Enabled on interface inside
 Total conns classified 1182, ingress 1182, egress 0
 Total whitelist classified 3, ingress 3, egress 0
 Total greylist classified 0, dropped 0, ingress 0, egress 0
 Total blacklist classified 1179, dropped 1000, ingress 1179, egress 0
```

The following is sample output from the **show dynamic-filter statistics interface outside detail** command:

```
ciscoasa# show dynamic-filter statistics interface outside detail
Enabled on interface outside
 Total conns classified 2108, ingress 2108, egress 0
 Total whitelist classified 0, ingress 0, egress 0
 Total greylist classified 1, dropped 1, ingress 0, egress 0
   Threat level 5 classified 1, dropped 1, ingress 0, egress 0
   Threat level 4 classified 0, dropped 0, ingress 0, egress 0
   ...
Total blacklist classified 30, dropped 20, ingress 11, egress 2
   Threat level 5 classified 6, dropped 6, ingress 4, egress 2
   Threat level 4 classified 5, dropped 5, ingress 5, egress 0
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.

Command	Description
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter updater-client	Shows information about the updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show dynamic-filter updater-client

To show information about the Botnet Traffic Filter updater server, including the server IP address, the next time the ASA will connect with the server, and the database version last installed, use the **show dynamic-filter updater-client** command in privileged EXEC mode.

show dynamic-filter updater-client

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following is sample output from the **show dynamic-filter updater-client** command:

```
ciscoasa# show dynamic-filter updater-client
Traffic Filter updater client is enabled
Updater server url is https://10.15.80.240:446
Application name: trafmon, version: 1.0
Encrypted UDI:
0bb93985f42d941e50dc8f022350d1a8de96ba6c1f6d45f4bc0ead02a7d5990be32f483b
5715cd80a215cedadd4e5ffe
Next update is in 00:02:00
Database file version is '907' fetched at 22:51:41 UTC Oct 16 2006,
size: 521408
```

Related Commands

Command	Description
address	Adds an IP address to the blacklist or whitelist.
clear configure dynamic-filter	Clears the running Botnet Traffic Filter configuration.
clear dynamic-filter dns-snoop	Clears Botnet Traffic Filter DNS snooping data.
clear dynamic-filter reports	Clears Botnet Traffic filter report data.

Command	Description
clear dynamic-filter statistics	Clears Botnet Traffic filter statistics.
dns domain-lookup	Enables the ASA to send DNS requests to a DNS server to perform a name lookup for supported commands.
dns server-group	Identifies a DNS server for the ASA.
dynamic-filter ambiguous-is-black	Treats greylisted traffic as blacklisted traffic for action purposes.
dynamic-filter blacklist	Edits the Botnet Traffic Filter blacklist.
dynamic-filter database fetch	Manually retrieves the Botnet Traffic Filter dynamic database.
dynamic-filter database find	Searches the dynamic database for a domain name or IP address.
dynamic-filter database purge	Manually deletes the Botnet Traffic Filter dynamic database.
dynamic-filter drop blacklist	Automatically drops blacklisted traffic.
dynamic-filter enable	Enables the Botnet Traffic Filter for a class of traffic or for all traffic if you do not specify an access list.
dynamic-filter updater-client enable	Enables downloading of the dynamic database.
dynamic-filter use-database	Enables use of the dynamic database.
dynamic-filter whitelist	Edits the Botnet Traffic Filter whitelist.
inspect dns dynamic-filter-snoop	Enables DNS inspection with Botnet Traffic Filter snooping.
name	Adds a name to the blacklist or whitelist.
show asp table dynamic-filter	Shows the Botnet Traffic Filter rules that are installed in the accelerated security path.
show dynamic-filter data	Shows information about the dynamic database, including when the dynamic database was last downloaded, the version of the database, how many entries the database contains, and 10 sample entries.
show dynamic-filter dns-snoop	Shows the Botnet Traffic Filter DNS snooping summary, or with the **detail** keyword, the actual IP addresses and names.
show dynamic-filter reports	Generates reports of the top 10 Botnet sites, ports, and infected hosts.
show dynamic-filter statistics	Shows how many connections were monitored with the Botnet Traffic Filter, and how many of those connections match the whitelist, blacklist, and greylist.
show running-config dynamic-filter	Shows the Botnet Traffic Filter running configuration.

show eigrp events

To display the EIGRP event log, use the **show eigrp events** command in privileged EXEC mode.

show eigrp [*as-number*] **events** [{ *start end* } **| type**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
end	(Optional) Limits the output to the entries with starting with the *start* index number and ending with the *end* index number.
start	(Optional) A number specifying the log entry index number. Specifying a start number causes the output to start with the specified event and end with the event specified by the *end* argument. Valid values are from 1 to 4294967295.
type	(Optional) Displays the events that are being logged.

Command Default

If a *start* and *end* is not specified, all log entries are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **show eigrp events** output displays up to 500 events. Once the maximum number of events has been reached, new events are added to the bottom of the output and old events are removed from the top of the output.

You can use the **clear eigrp events** command to clear the EIGRP event log.

The **show eigrp events type** command displays the logging status of EIGRP events. By default, neighbor changes, neighbor warning, and DUAL FSM messages are logged. You can disable neighbor change event logging using the **no eigrp log-neighbor-changes** command. You can disable neighbor warning event logging using the **no eigrp log-neighbor-warnings** command. You cannot disable the logging of DUAL FSM events.

Examples

The following is sample output from the **show eigrp events** command:

```
ciscoasa# show eigrp events
Event information for AS 100:
1    12:11:23.500 Change queue emptied, entries: 4
2    12:11:23.500 Metric set: 10.1.0.0/16 53760
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
9    12:11:23.500 Rcv update met/succmet: 53760 28160
10   12:11:23.500 Rcv update dest/nh: 10.1.0.0/16 10.130.60.248
11   12:11:23.500 Metric set: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command with a start and stop number defined:

```
ciscoasa# show eigrp events 3 8
Event information for AS 100:
3    12:11:23.500 Update reason, delay: new if 4294967295
4    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
5    12:11:23.500 Update reason, delay: metric chg 4294967295
6    12:11:23.500 Update sent, RD: 10.1.0.0/16 4294967295
7    12:11:23.500 Route install: 10.1.0.0/16 10.130.60.248
8    12:11:23.500 Find FS: 10.1.0.0/16 4294967295
```

The following is sample output from the **show eigrp events** command when there are no entries in the EIGRP event log:

```
ciscoasa# show eigrp events
Event information for AS 100:  Event log is empty.
```

The following is sample output from the **show eigrp events type** command:

```
ciscoasa# show eigrp events type
EIGRP-IPv4 Event Logging for AS 100:
      Log Size          500
      Neighbor Changes  Enable
      Neighbor Warnings Enable
      Dual FSM          Enable
```

Related Commands

Command	Description
clear eigrp events	Clears the EIGRP event logging buffer.
eigrp log-neighbor-changes	Enables the logging of neighbor change events.
eigrp log-neighbor-warnings	Enables the logging of neighbor warning events.

show eigrp interfaces

To display the interfaces participating in EIGRP routing, use the **show eigrp interfaces** command in privileged EXEC mode.

show eigrp [*as-number*] **interfaces** [*if-name*] [**detail**]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are displaying active interfaces. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail information.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name limits the display to the specified interface.

Command Default

If you do not specify an interface name, information for all EIGRP interfaces is displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **show eigrp interfaces** command to determine on which interfaces EIGRP is active, and to learn information about EIGRP relating to those interfaces.

If an interface is specified, only that interface is displayed. Otherwise, all interfaces on which EIGRP is running are displayed.

If an autonomous system is specified, only the routing process for the specified autonomous system is displayed. Otherwise, all EIGRP processes are displayed.

Examples

The following is sample output from the **show eigrp interfaces** command:

```
ciscoasa# show eigrp interfaces
EIGRP-IPv4 interfaces for process 100
                    Xmit Queue    Mean   Pacing Time   Multicast   Pending
```

```
Interface    Peers   Un/Reliable   SRTT   Un/Reliable   Flow Timer  Routes
mgmt           0         0/0          0      11/434          0          0
outside        1         0/0        337       0/10           0          0
inside         1         0/0         10       1/63         103          0
```

Table 6-2 describes the significant fields shown in the display.

Table 43: show eigrp interfaces Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Peers	Number of directly-connected peers.
Xmit Queue Un/Reliable	Number of packets remaining in the Unreliable and Reliable transmit queues.
Mean SRTT	Mean smooth round-trip time interval (in seconds).
Pacing Time Un/Reliable	Pacing time (in seconds) used to determine when EIGRP packets should be sent out the interface (unreliable and reliable packets).
Multicast Flow Timer	Maximum number of seconds in which the ASA will send multicast EIGRP packets.
Pending Routes	Number of routes in the packets in the transmit queue waiting to be sent.

Related Commands

Command	Description
network	Defines the networks and interfaces that participate in the EIGRP routing process.

show eigrp neighbors

To display the EIGRP neighbor table, use the **show eigrp neighbors** command in privileged EXEC mode.

show eigrp [*as-number*] **neighbors** [**detail | static**] [*if-name*]

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are deleting neighbor entries. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
detail	(Optional) Displays detail neighbor information.
if-name	(Optional) The name of an interface as specified by the **nameif** command. Specifying an interface name displays all neighbor table entries that were learned through that interface.
static	(Optional) Displays EIGRP neighbors that are statically defined using the **neighbor** command.

Command Default

If you do not specify an interface name, the neighbors learned through all interfaces are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can use the **clear eigrp neighbors** command to clear the dynamically learned neighbors from the EIGRP neighbor table.

Static neighbors are not included in the output unless you use the **static** keyword.

Examples

The following is sample output from the **show eigrp neighbors** command:

```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 Neighbors for process 100
Address                 Interface      Holdtime Uptime   Q      Seq  SRTT  RTO
                                       (secs)   (h:m:s)  Count  Num  (ms)  (ms)
172.16.81.28            Ethernet1      13       0:00:41  0      11   4     20
```

```
172.16.80.28            Ethernet0     14        0:02:01  0       10    12     24
172.16.80.31            Ethernet0     12        0:02:02  0       4     5      20
```

Table 6-2 describes the significant fields shown in the display.

Table 44: show eigrp neighbors Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the ASA receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the ASA waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor. If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed. If this value reaches 0, the ASA considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the ASA first heard from this neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the ASA is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the ASA to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the ASA waits before resending a packet from the retransmission queue to a neighbor.

The following is sample output from the **show eigrp neighbors static** command:

```
ciscoasa# show eigrp neighbors static
EIGRP-IPv4 neighbors for process 100
Static Address                  Interface
192.168.1.5                     management
```

Table 6-4 describes the significant fields shown in the display.

Table 45: show ip eigrp neighbors static Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Static Address	IP address of the EIGRP neighbor.
Interface	Interface on which the ASA receives hello packets from the neighbor.

Examples

The following is sample output from the **show eigrp neighbors detail** command:

```
ciscoasa# show eigrp neighbors detail
EIGRP-IPv4 neighbors for process 100
H   Address                 Interface       Hold Uptime   SRTT   RTO  Q Seq Tye
                                            (sec)         (ms)       Cnt Num
3   1.1.1.3                 Et0/0             12 00:04:48 1832   5000  0  14
   Version 12.2/1.2, Retrans: 0, Retries: 0
   Restart time 00:01:05
0   10.4.9.5                Fa0/0             11 00:04:07  768   4608  0  4   S
   Version 12.2/1.2, Retrans: 0, Retries: 0
2   10.4.9.10               Fa0/0             13 1w0d        1   3000  0  6   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
1   10.4.9.6                Fa0/0             12 1w0d        1   3000  0  4   S
   Version 12.2/1.2, Retrans: 1, Retries: 0
```

Table 46: show ip eigrp neighbors details Field Descriptions describes the significant fields shown in the display.

Table 46: show ip eigrp neighbors details Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
H	This column lists the order in which a peering session was established with the specified neighbor. The order is specified with sequential numbering starting with 0.
Address	IP address of the EIGRP neighbor.
Interface	Interface on which the ASA receives hello packets from the neighbor.
Holdtime	Length of time (in seconds) that the ASA waits to hear from the neighbor before declaring it down. This hold time is received from the neighbor in the hello packet, and begins decreasing until another hello packet is received from the neighbor. If the neighbor is using the default hold time, this number will be less than 15. If the peer configures a non-default hold time, the non-default hold time will be displayed. If this value reaches 0, the ASA considers the neighbor unreachable.
Uptime	Elapsed time (in hours:minutes: seconds) since the ASA first heard from this neighbor.
SRTT	Smooth round-trip time. This is the number of milliseconds required for an EIGRP packet to be sent to this neighbor and for the ASA to receive an acknowledgment of that packet.
RTO	Retransmission timeout (in milliseconds). This is the amount of time the ASA waits before resending a packet from the retransmission queue to a neighbor.
Q Count	Number of EIGRP packets (update, query, and reply) that the ASA is waiting to send.
Seq Num	Sequence number of the last update, query, or reply packet that was received from the neighbor.
Version	The software version that the specified peer is running.
Retrans	The number of times that a packet has been retransmitted.

Field	Description
Retries	The number of times an attempt was made to retransmit a packet.
Restart time	Elapsed time (in hours:minutes:seconds) since the specified neighbor has restarted.

Related Commands

Command	Description
clear eigrp neighbors	Clears the EIGRP neighbor table.
debug eigrp neighbors	Displays EIGRP neighbor debugging messages.
debug ip eigrp	Displays EIGRP packet debugging messages.

show eigrp topology

To display the EIGRP topology table, use the **show eigrp topology** command in privileged EXEC mode.

show eigrp [*as-number*] **topology** [*ip-addr* [*mask*] **| active | all-links | pending | summary | zero-successors**]

Syntax Description

active	(Optional) Displays only active entries in the EIGRP topology table.
all-links	(Optional) Displays all routes in the EIGRP topology table, even those that are not feasible successors.
as-number	(Optional) Specifies the autonomous system number of the EIGRP process. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.
ip-addr	(Optional) Defines the IP address from the topology table to display. When specified with a mask, a detailed description of the entry is provided.
mask	(Optional) Defines the network mask to apply to the *ip-addr* argument.
pending	(Optional) Displays all entries in the EIGRP topology table that are waiting for an update from a neighbor or are waiting to reply to a neighbor.
summary	(Optional) Displays a summary of the EIGRP topology table.
zero-successors	(Optional) Displays available routes in the EIGRP topology table.

Command Default

Only routes that are feasible successors are displayed. Use the **all-links** keyword to display all routes, including those that are not feasible successors.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can use the **clear eigrp topology** command to remove the dynamic entries from the topology table.

Examples

The following is sample output from the **show eigrp topology** command:

Command History

```
EIGRP-IPv4 Topology Table for AS(100)/ID(192.168.1.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - Reply status
P 10.2.1.0 255.255.255.0, 2 successors, FD is 0
          via 10.16.80.28 (46251776/46226176), Ethernet0
          via 10.16.81.28 (46251776/46226176), Ethernet1
P 10.2.1.0 255.255.255.0, 1 successors, FD is 307200
          via Connected, Ethernet1
          via 10.16.81.28 (307200/281600), Ethernet1
          via 10.16.80.28 (307200/281600), Ethernet0
```

Table 6-6 describes the significant fields shown in the displays.

Table 47: show eigrp topology Field Information

Field	Description
Codes	State of this topology table entry. Passive and Active refer to the EIGRP state with respect to this destination; Update, Query, and Reply refer to the type of packet that is being sent.
P - Passive	The route is known to be good and no EIGRP computations are being performed for this destination.
A - Active	EIGRP computations are being performed for this destination.
U - Update	Indicates that an update packet was sent to this destination.
Q - Query	Indicates that a query packet was sent to this destination.
R - Reply	Indicates that a reply packet was sent to this destination.
r - Reply status	Flag that is set after the software has sent a query and is waiting for a reply.
address mask	Destination IP address and mask.
successors	Number of successors. This number corresponds to the number of next hops in the IP routing table. If “successors” is capitalized, then the route or next hop is in a transition state.
FD	Feasible distance. The feasible distance is the best metric to reach the destination or the best metric that was known when the route went active. This value is used in the feasibility condition check. If the reported distance of the router (the metric after the slash) is less than the feasible distance, the feasibility condition is met and that path is a feasible successor. Once the software determines it has a feasible successor, it need not send a query for that destination.
via	IP address of the peer that told the software about this destination. The first *n* of these entries, where *n* is the number of successors, is the current successors. The remaining entries on the list are feasible successors.
(*cost* /*adv_cost*)	The first number is the EIGRP metric that represents the cost to the destination. The second number is the EIGRP metric that this peer advertised.

Field	Description
interface	The interface from which the information was learned.

Command History

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an internal route.

```
ciscoasa# show eigrp topology 10.2.1.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.2.1.0
255.255.255.0
 State is Passive, Query origin flag is 1, 1 Successor(s), FD is 281600
 Routing Descriptor Blocks:
  0.0.0.0 (Ethernet0/0), from Connected, Send flag is 0x0
   Composite metric is (281600/0), Route is Internal
   Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 1000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 0
```

The following is sample output from the **show eigrp topology** used with an IP address. The output shown is for an external route.

```
ciscoasa# show eigrp topology 10.4.80.0 255.255.255.0
EIGRP-IPv4 (AS 100): Topology Default-IP-Routing-Table(0) entry for entry for 10.4.80.0
255.255.255.0
 State is Passive, Query origin flag is 1, 1 Successor(s), FD is 409600
 Routing Descriptor Blocks:
  10.2.1.1 (Ethernet0/0), from 10.2.1.1, Send flag is 0x0
   Composite metric is (409600/128256), Route is External
   Vector metric:
    Minimum bandwidth is 10000 Kbit
    Total delay is 6000 microseconds
    Reliability is 255/255
    Load is 1/255
    Minimum MTU is 1500
    Hop count is 1
   External data:
    Originating router is 10.89.245.1
    AS number of route is 0
    External protocol is Connected, external metric is 0
    Administrator tag is 0 (0x00000000)
```

Related Commands

Command	Description
clear eigrp topology	Clears the dynamically discovered entries from the EIGRP topology table.

show eigrp traffic

To display the number of EIGRP packets sent and received, use the **show eigrp traffic** command in privileged EXEC mode.

show eigrp [*as-number*] **traffic**

Syntax Description

as-number	(Optional) Specifies the autonomous system number of the EIGRP process for which you are viewing the event log. Because the ASA only supports one EIGRP routing process, you do not need to specify the autonomous system number.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

You can use the **clear eigrp traffic** command to clear the EIGRP traffic statistics.

Examples

The following is sample output from the **show eigrp traffic** command:

```
ciscoasa# show eigrp traffic
EIGRP-IPv4 Traffic Statistics for AS 100
  Hellos sent/received: 218/205
  Updates sent/received: 7/23
  Queries sent/received: 2/0
  Replies sent/received: 0/2
  Acks sent/received: 21/14
  Input queue high water mark 0, 0 drops
  SIA-Queries sent/received: 0/0
  SIA-Replies sent/received: 0/0
  Hello Process ID: 1719439416
  PDM Process ID: 1719439824
```

Table 6-4 describes the significant fields shown in the display.

Table 48: show eigrp traffic Field Descriptions

Field	Description
process	Autonomous system number for the EIGRP routing process.
Hellos sent/received	Number of hello packets sent and received.
Updates sent/received	Number of update packets sent and received.
Queries sent/received	Number of query packets sent and received.
Replies sent/received	Number of reply packets sent and received.
Acks sent/received	Number of acknowledgment packets sent and received.
Input queue high water mark/drops	Number of received packets that are approaching the maximum receive threshold and number of dropped packets.
SIA-Queries sent/received	Stuck-in-active queries sent and received.
SIA-Replies sent/received	Stuck-in-active replies sent and received.

Related Commands

Command	Description
debug eigrp packets	Displays debugging information for EIGRP packets sent and received.
debug eigrp transmit	Displays debugging information for EIGRP messages sent.

show environment

To display system environment information for system components, use the **show environment** command in privileged EXEC mode.

show environment [**alarm-contact | driver | fans | power-consumption | power-supply | temperature**] [**chassis | cpu | voltage**]

Syntax Description

alarm-contact	(Optional) Displays the operational status of the input alarm contacts on an ISA 3000 device.
chassis	(Optional) Limits the temperature display to the chassis.
cpu	(Optional) Limits the temperature display to the processors.
driver	(Optional) Displays the environment monitoring (IPMI) driver status. The driver status can be one of the following: • RUNNING—The driver is operational. • STOPPED—An error has caused the driver to stop.
fans	(Optional) Displays the operational status of the cooling fans. The status is one of the following: • OK—The fan is operating normally. • Failed—The fan has failed and should be replaced. When you remove dual fan module, to view the actual status of the fan, use the **show environment basic** and **show environment expand** FXOS commands.
power-consumption	(Optional) Shows the power consumption for PoE interfaces.

power-supply	(Optional) Displays the operational status of the power supplies. The status for each power supply is one of the following: • OK—The power supply is operating normally. • Failed—The power supply has failed and should be replaced. • Not Present—The specified power supply is not installed. The power supply redundancy status also displays. The redundancy status is one of the following: • OK—The unit is operating normally with full resources. • Lost—The unit has lost redundancy but is operating normally with minimum resources. Any further failures will result in a system shutdown. • N/A—The unit is not configured for power supply redundancy.
temperature	(Optional) Displays the temperature and status of the processors and chassis. The temperature is given in celsius. The status is one of the following: • OK—The temperature is within normal operating range. • Critical—The temperature is outside of normal operating range.
voltage	(Optional) Displays the values for CPU voltage channels 1-24. Excludes the operational status.

Command Default

All operational information, except for the driver, is displayed if no keywords are specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.1(1)	This command was added.
8.4(2)	The output for an ASA 5585-X SSP was added. In addition, support for a dual SSP installation was added.
8.4.4(1)	Displayed power supply temperature values for the ASA 5515-X, ASA 5525-X, 5545-X, and ASA 5555-X have been changed in the output.
8.6(1)	The output for CPU voltage regulator thermal events in the ASA 5545-X and ASA 5555-X was added. The output for power supply input status was added. The output for voltage sensors was added.
9.7(1)	We added the **alarm-contact** keyword for the ISA 3000.
9.13(1)	We added the **power-consumption** keyword for the Firepower 1010 PoE interfaces.

Usage Guidelines

You can display operating environment information for the physical components in the device. This information includes the operational status of the fans and power supplies, and temperature and status of the CPUs and chassis. For ISA 3000 devices, it includes information about the input alarm contacts.

Note For a dual SSP installation, only the sensors for the chassis master show output for the cooling fans and power supplies.

Examples

The following is sample generic output from the **show environment** command:

```
ciscoasa# show environment

Cooling Fans:
-----------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan) Power Supplies:
-----------------------------------
   Power Supply Unit Redundancy: OK
   Temperature:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
   Cooling Fans:
   --------------------------------
   Left Slot (PS0): 6900 RPM - OK  (Power Supply Fan)
   Right Slot (PS1): 7000 RPM - OK  (Power Supply Fan)
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 44.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 45.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 28.0 C - OK  (Chassis Front Temperature)
   Ambient 2: 40.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 28.0 C - OK  (CPU1 Front Temperature)
   Ambient 4: 36.50 C - OK  (CPU1 Back Temperature)
   Ambient 5: 34.50 C - OK  (CPU2 Front Temperature)
   Ambient 6: 43.25 C - OK  (CPU2 Back Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 26 C - OK  (Power Supply Temperature)
   Right Slot (PS1): 27 C - OK  (Power Supply Temperature)
```

The following is sample output from the **show environment driver** command:

```
ciscoasa# show environment driver
Cooling Fans:
-----------------------------------
   Chassis Fans:
   --------------------------------
   Cooling Fan 1: 5888 RPM - OK
   Cooling Fan 2: 5632 RPM - OK
   Cooling Fan 3: 5888 RPM - OK
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Power Supplies:
-----------------------------------
   Left Slot (PS0): Not Present
   Right Slot (PS1): Present
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
   Left Slot (PS0): N/A
   Right Slot (PS1): 8448 RPM - OK
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 70.0 C - OK
   Chassis:
   --------------------------------
   Ambient 1: 36.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 31.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 39.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): N/A
   Right Slot (PS1): 33 C - OK
Voltage:
-----------------------------------
   Channel 1:  1.168 V -  (CPU Core 0.46V-1.4V)
   Channel 2: 11.954 V -  (12V)
   Channel 3:  4.998 V -  (5V)
   Channel 4:  3.296 V -  (3.3V)
   Channel 5:  1.496 V -  (DDR3 1.5V)
   Channel 6:  1.048 V -  (PCH 1.5V)
```

The following is sample output from the **show environment** command for an ASA 5555-X:

```
ciscoasa# show environment
Cooling Fans:
-----------------------------------
   Chassis Fans:
   --------------------------------
   Power Supplies:
```

```
   --------------------------------
   Left Slot (PS0): 9728 RPM - OK
   Right Slot (PS1): 0 RPM - OK
Power Supplies:
 -----------------------------------

    Left Slot (PS0): Present
    Right Slot (PS1): Present

    Power Input:
    --------------------------------
    Left Slot (PS0): OK
    Right Slot (PS1): Failure Detected
    Temperature:
    --------------------------------
    Left Slot (PS0): 29 C - OK
    Right Slot (PS1): N/A
   Processors:
   --------------------------------
   Processor 1: 81.0 C - OK
   Chassis:
   --------------------------------
   Ambient 1: 39.0 C - OK  (Chassis Back Temperature)
   Ambient 2: 32.0 C - OK  (Chassis Front Temperature)
   Ambient 3: 47.0 C - OK  (Chassis Back Left Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 33 C - OK
   Right Slot (PS1): -128 C - OK
```

The following is sample output from the **show environment** command for an ASA 5585-X chassis master in a dual SSP installation:

```
ciscoasa(config)# show environment
Cooling Fans:
-----------------------------------
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)
Power Supplies:
-----------------------------------
   Power Supply Unit Redundancy: N/A
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 7000 RPM - OK  (Fan Module Fan)
   Right Slot (PS1): 6900 RPM - OK  (Power Supply Fan)
Temperature:
-----------------------------------
   Processors:
   --------------------------------
   Processor 1: 48.0 C - OK  (CPU1 Core Temperature)
   Processor 2: 47.0 C - OK  (CPU2 Core Temperature)
   Chassis:
   --------------------------------
   Ambient 1: 25.5 C - OK  (Chassis Front Temperature)
   Ambient 2: 37.5 C - OK  (Chassis Back Temperature)
   Ambient 3: 31.50 C - OK  (CPU1 Back Temperature)
   Ambient 4: 27.75 C - OK  (CPU1 Front Temperature)
   Ambient 5: 38.25 C - OK  (CPU2 Back Temperature)
   Ambient 6: 34.0 C - OK  (CPU2 Front Temperature)
   Power Supplies:
   --------------------------------
   Left Slot (PS0): 64 C - OK  (Fan Module Temperature)
   Right Slot (PS1): 64 C - OK  (Power Supply Temperature)
Voltage:
-----------------------------------
   Channel 1:  3.310 V -  (3.3V (U142 VX1))
   Channel 2:  1.492 V -  (1.5V (U142 VX2))
   Channel 3:  1.053 V -  (1.05V (U142 VX3))
   Channel 4:  3.328 V -  (3.3V_STDBY (U142 VP1))
   Channel 5: 11.675 V -  (12V (U142 VP2))
   Channel 6:  4.921 V -  (5.0V (U142 VP3))
   Channel 7:  6.713 V -  (7.0V (U142 VP4))
   Channel 8:  9.763 V -  (IBV (U142 VH))
   Channel 9:  1.048 V -  (1.05VB (U209 VX2))
   Channel 10:  1.209 V -  (1.2V (U209 VX3))
   Channel 11:  1.109 V -  (1.1V (U209 VX4))
   Channel 12:  0.999 V -  (1.0V (U209 VX5))
   Channel 13:  3.324 V -  (3.3V STDBY (U209 VP1))
   Channel 14:  2.504 V -  (2.5V (U209 VP2))
   Channel 15:  1.799 V -  (1.8V (U209 VP3))
   Channel 16:  1.899 V -  (1.9V (U209 VP4))
   Channel 17:  9.763 V -  (IBV (U209 VH))
   Channel 18:  2.048 V -  (VTT CPU0 (U83 VX2))
   Channel 19:  2.048 V -  (VTT CPU1 (U83 VX3))
   Channel 20:  2.048 V -  (VCC CPU0 (U83 VX4))
   Channel 21:  2.048 V -  (VCC CPU1 (U83 VX5))
   Channel 22:  1.516 V -  (1.5VA (U83 VP1))
   Channel 23:  1.515 V -  (1.5VB (U83 VP2))
   Channel 24:  8.937 V -  (IBV (U83 VH))
```

If the ASA was shut down because of a CPU voltage regulator thermal event, the following warning message appears:

```
WARNING: ASA was previously shut down due to a CPU Voltage Regulator running beyond the max
 thermal operating temperature. The chassis and CPU need to be inspected immediately for
ventilation issues.
```

For more information, see syslog message 735024 in the syslog messages guide.

The following is a sample output from the show environment alarm-contact command:

```
ciscoasa> show environment alarm-contact
ALARM CONTACT 1
   Status:      not asserted
   Description: external alarm contact 1
   Severity:    minor
   Trigger:     closed
ALARM CONTACT 2
   Status:      not asserted
   Description: external alarm contact 2
   Severity:    minor
   Trigger:     closed
```

The following is a sample of driver error statistics.

```
Driver Error Statistics:
-------------------------
I2C I/O Errors          : 0
GPIO Errors             : 0
Ioctl Null Ptr Errors   : 0
```

```
Poll Errors             : 0
Invalid Ioctl Errors    : 0
PECI Errors             : 3
Unknown Errors          : 0
```

The PECI Errors indicate that there is an issue when retrieving the CPU temperature data. The error count number is the number of times it failed retrieving the temperature data.

Related Commands

Command	Description
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.
show facility-alarm relay	Displays status information for triggered alarms.
show version	Displays the hardware and software version.

show event manager

To show information about each configured event manager applet, use the **show event manager** command in privileged EXEC mode.

show event manager

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Examples

The following is sample output from the **show event manager** command:

```
ciscoasa# show event manager
event manager applet 21, hits 1, last 2014/01/19 06:47:46
  last file disk0:/eem-21-20140119-064746.log
  event countdown 21 secs, left 0 secs, hits 1, last 2014/01/19 06:47:47
  action 1 cli command "sh ver", hits 1, last 2014/01/19 06:47:46
```

Related Commands

Command	Description
show running-config event manager	Shows the event manager running configuration.

show f – show ipu

show facility-alarm

To display the triggered alarms in an ISA 3000 device, use the **show facility-alarm** command in user EXEC mode.

show facility-alarm { **relay** | **status** [**info** | **major** | **minor**] }

Syntax Description

relay	Displays the alarms that have energized the alarm output relay.
status [**info** | **major** | **minor**]	Displays all the alarms that have been triggered. You can add the following keywords to limit the list: • **major**—Displays all the major severity alarms. • **minor**—Displays all the minor severity alarms. • **info**—Displays all the alarms. This keyword provides the same output as using no keyword.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	We introduced this command.

Usage Guidelines

Use the **relay** keyword to view just the alarms that have energized the alarm output relay. The output alarm relay is energized based on whether you configure the triggered alarms to activate it. Energizing the alarm output relay activates the device that you attach to it, such as a flashing light or buzzer.

Use the **status** keyword to view all the alarms that have been triggered, regardless of whether the alarm action triggered the external alarm output relay.

The following table explains the columns in the output.

Column	Description
Source	The device from which the alarm was triggered. This is usually the hostname configured on the device.

Column	Description
Severity	Major or minor.
Description	The type of alarm triggered. For example, temperature, external alarm contact, or redundant power supply.
Relay	Whether the external alarm output relay was energized or de-energized. The external output alarm is triggered based on your alarm configuration.
Time	The timestamp of the triggered alarm.

Examples

The following is a sample output from the **show facility-alarm relay** command:

```
ciscoasa> show facility-alarm relay

Source    Severity   Description                         Relay      Time
ciscoasa  minor      external alarm contact 1 triggered  Energized  06:56:50 UTC Mon Sep
22 2014
```

The following is a sample output from the **show facility-alarm status** command:

```
ciscoasa> show facility-alarm status info

Source    Severity  Description                       Relay         Time
ciscoasa minor external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep 22
2014
ciscoasa minor Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep 22
2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014
ciscoasa major Redundant pwr missing or failed     De-energized  07:00:19 UTC Mon Sep 22
2014
ciscoasa> show facility-alarm status major
Source    Severity  Description                       Relay         Time
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014
ciscoasa  major     Redundant pwr missing or failed   De-energized  07:00:19 UTC Mon Sep
22 2014
ciscoasa> show facility-alarm status minor
Source    Severity  Description                         Relay         Time
ciscoasa  minor     external alarm contact 1 triggered  Energized     06:56:50 UTC Mon Sep
 22 2014
ciscoasa  minor     Temp below Secondary Threshold      De-energized  06:56:49 UTC Mon Sep
 22 2014
```

Related Commands

Command	Description
alarm contact description	Specifies the description for the alarm inputs.
alarm contact severity	Specifies the severity of alarms.
alarm contact trigger	Specifies a trigger for one or all alarm inputs.
alarm facility input-alarm	Specifies the logging and notification options for alarm inputs.

Command	Description
alarm facility power-supply rps	Configures the power supply alarms.
alarm facility temperature	Configures the temperature alarms.
alarm facility temperature (high and low thresholds)	Configures the low or high temperature threshold value.
show alarm settings	Displays all global alarm settings.
show environment alarm-contact	Displays the status of the input alarm contacts.
clear facility-alarm output	De-energizes the output relay and clears the alarm state of the LED.

show failover

To display information about the failover status of the unit, use the **show failover** command in privileged EXEC mode.

show failover [**descriptor**] [**exec**] [**group** *num* **| history** [**details**] | **interface** | **state** | **trace** [*options*] | [**statistics** [**all** | **events** | **unit** | **np-clients** | **cp-clients** | **bulk-sync** [**all** | **control-plane** | **data-plane** |] | **interface** [**all**]] | **details**] [**config-sync**]

Syntax Description

descriptor	Shows failover interface descriptors in the form of two numbers for every interface. When exchanging information about an interface, this unit uses the first number in the messages it sends to its peer. And it expects the second number in the messages it receives from its peer.
details	Displays the failover details of the pairs in a high availability pair.
exec	Shows failover command execution information.
group	Displays the running state of the specified failover group.
history [details]	Displays failover history. The failover history displays past failover state changes and the reason for the state change for the active unit. The failover history includes the failure reason along with its specific details; this helps with troubleshooting. Add the details keyword to display failover history from the peer unit. This includes failover state changes and the reason for the state change, for the peer unit. History information is cleared when the device reboots.
interface	Displays failover and stateful link information.
num	Failover group number.
state	Displays the failover state of both the failover units. The information displayed includes the primary or secondary status of the unit, the Active/Standby status of the unit, and the last reported reason for failover. The fail reason remains in the output even when the reason for failure is cleared.
trace [*options*]	(Optional) Shows the failover event trace. Options include to show the failover event trace by levels (1-5): • **critical** — to filter failover critical event trace (level = 1) • **debugging**— to filter failover debugging trace (Debug level = 5) • **error**— to filter failover internal exception (level = 2) • **informational**— to filter failover informational trace (level = 4) • **warning**— to filter failover warnings (level = 3)

statistics [**all** | **events** | **unit** | **np-clients** | **cp-clients** | **bulk-sync**	Displays transmit and receive packet count of failover command interface. • **np-clients**—displays the HA data-path client's packet's statistics. • **cp-clients**—displays the HA control plane client's packet's statistics. • **bulk-sync**—displays the sync time for the HA data-plane clients and control-plane clients. • **events**—displays the local failures notified by App agent—HA LAN link uptime, Supervisor's heartbeat failures, and Disk full issues. • **all**—displays the consolidated failover statistics for interface, np-client, cp-client, and bulk-sync.
details	Displays the failover details of the pairs in a high availability pair.
config-sync	Displays device configuration, device status, and checksum details about the Config-Sync Optimization feature.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.1(6)	The **details** keyword was added.
7.0(1)	This command was modified. The output includes additional information.
8.2(2)	This command was modified. The output includes IPv6 addresses for firewall and failover interfaces. The Stateful Failover statistics output includes information for the IPv6 neighbor discover table (IPv6 ND tbl) updates.
9.9.2	This command was modified. The failover history output includes enhancements to the failure reasons. The history details keyword was added. This displays failover history from the peer unit.
9.16(1)	The **details** keyword was added
9.18(1)	The **config-sync** keyword was added.
9.20(2)	The **statistics all**,**statistics events**,**statistics np-clients**,**statistics cp-clients**, and **statistics bulk-sync** keywords were added.

Usage Guidelines

The **show failover** command displays the dynamic failover information, interface status, and Stateful Failover statistics.

If both IPv4 and IPv6 addresses are configured on an interface, both addresses appear in the output. Because an interface can have more than one IPv6 address configured on it, only the link-local address is displayed. If there is no IPv4 address configured on the interface, the IPv4 address in the output appears as 0.0.0.0. If there is no IPv6 address configured on an interface, the address is simply omitted from the output.

The Stateful Failover Logical Update Statistics output appears only when Stateful Failover is enabled. The “xerr” and “rerr” values do not indicate errors in failover, but rather the number of packet transmit or receive errors.

Note Stateful Failover, and therefore Stateful Failover statistics output, is not available on the ASA 5505.

In the **show failover** command output, the stateful failover fields have the following values:

- Stateful Obj has these values:
  - xmit—Indicates the number of packets transmitted.
  - xerr—Indicates the number of transmit errors.
  - rcv—Indicates the number of packets received.
  - rerr—Indicates the number of receive errors.
- Each row is for a particular object static count as follows:
  - General—Indicates the sum of all stateful objects.
  - sys cmd—Refers to the logical update system commands, such as login or stay alive.
  - up time—Indicates the value for the ASA up time, which the active ASA passes on to the standby ASA.
  - RPC services—Remote Procedure Call connection information.
  - TCP conn—Dynamic TCP connection information.
  - UDP conn—Dynamic UDP connection information.
  - ARP tbl—Dynamic ARP table information.
  - Xlate_Timeout—Indicates connection translation timeout information.
  - IPv6 ND tbl—The IPv6 neighbor discovery table information.
  - VPN IKE upd—IKE connection information.
  - VPN IPSEC upd—IPsec connection information.
  - VPN CTCP upd—cTCP tunnel connection information.
  - VPN SDI upd—SDI AAA connection information.
  - VPN DHCP upd—Tunneled DHCP connection information.
  - SIP Session—SIP signalling session information.

- Route Session—LU statistics of the route synhronization updates

If you do not enter a failover IP address, the **show failover** command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remain in a “waiting” state. You must set a failover IP address for failover to work.

Table 7-1 describes the interface states for failover.

Table 49: Failover Interface States

State	Description
Normal	The interface is up and receiving hello packets from the corresponding interface on the peer unit.
Normal (Waiting)	The interface is up but has not yet received a hello packet from the corresponding interface on the peer unit. Verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces. You can also see this state when the failover interface goes down.
Normal (Not-Monitored)	The interface is up but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
No Link	The physical link is down.
No Link (Waiting)	The physical link is down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After restoring the link, verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
No Link (Not-Monitored)	The physical link is down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Link Down	The physical link is up, but the interface is administratively down.
Link Down (Waiting)	The physical link is up, but the interface is administratively down and the interface has not yet received a hello packet from the corresponding interface on the peer unit. After bringing the interface up (using the **no shutdown** command in interface configuration mode), verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
Link Down (Not-Monitored)	The physical link is up, but the interface is administratively down but is not monitored by the failover process. The failure of an interface that is not monitored does not trigger failover.
Testing	The interface is in testing mode due to missed hello packets from the corresponding interface on the peer unit.
Failed	Interface testing has failed and the interface is marked as failed. If the interface failure causes the failover criteria to be met, then the interface failure causes a failover to the secondary unit or failover group.

Usage Guidelines

In multiple context mode, only the **show failover** command is available in a security context; you cannot enter the optional keywords.

Examples

The following is sample output from the **show failover** command for Active/Standby Failover. The ASAs use IPv6 addresses on the failover link (folink) and the inside interface.

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/4 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 3 of 1049 maximum
MAC Address Move Notification Interval not set
Version: Ours 98.1(1)86, Mate 98.1(1)86
Serial Number: Ours JAF1610APKQ, Mate JAF1610ALGM
Last Failover at: 12:52:34 UTC Apr 26 2017
        This host: Primary - Active
                Active time: 87 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.1): Normal (Monitored)
                  Interface outside (192.168.77.1): No Link (Waiting)
                  Interface dmz (192.168.67.1): No Link (Waiting)
                slot 1: empty
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5585-SSP-10 hw/sw rev (2.0/98.1(1)86) status (Up Sys)
                  Interface inside (10.86.118.2): Normal (Waiting)
                  Interface outside (192.168.77.2): No Link (Waiting)
                  Interface dmz (192.168.67.2): No Link (Waiting)
                slot 1: empty
                slot 1: empty
Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/4 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         22         0          6          0
        sys cmd         6          0          6          0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         14         0          0          0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     0          0          0          0
        VPN IKEv1 SA    0          0          0          0
        VPN IKEv1 P2    0          0          0          0
        VPN IKEv2 SA    0          0          0          0
        VPN IKEv2 P2    0          0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
        SIP Session     0          0          0          0
        SIP Tx  0          0          0          0
        SIP Pinhole     0          0          0          0
        Route Session   0          0          0          0
        Router ID       1          0          0          0
        User-Identity   1          0          0          0
        CTS SGTNAME     0          0          0          0
        CTS PAC         0          0          0          0
        TrustSec-SXP    0          0          0          0
        IPv6 Route      0          0          0          0
        STS Table       0          0          0          0
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       5       6
        Xmit Q:         0       27      86
```

The following is sample output from the **show failover** command for Active/Active Failover. In this example, only the admin context has IPv6 addresses assigned to the interfaces.

```
ciscoasa# show failover
Failover On
Failover unit Primary
Failover LAN Interface: folink GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004
  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)
                slot 0: ASA-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.5): Normal
                admin Interface folink (10.132.9.5/fe80::2a0:c9ff:fe03:101): Normal
                admin Interface inside (10.130.8.5/fe80::2a0:c9ff:fe01:101): Normal
                admin Interface fourth (10.130.9.5/fe80::3eff:fe11:6670): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal
  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)
                slot 0: ASA-5545 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                admin Interface outside (10.132.8.6): Normal
                admin Interface folink (10.132.9.6/fe80::2a0:c9ff:fe03:102): Normal
                admin Interface inside (10.130.8.6/fe80::2a0:c9ff:fe01:102): Normal
                admin Interface fourth (10.130.9.6/fe80::3eff:fe11:6671): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal
Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        IPv6 ND tbl     22         0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0
  SIP Session    0          0          0          0
        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

The following is sample output from the **show failover** command on the ASA 5505:

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006
        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

The following is sample output from the **show failover state** command for an active-active setup:

```
ciscoasa(config)# show failover state
               State          Last Failure Reason      Date/Time
This host  -   Secondary
    Group 1    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
    Group 2    Failed         Backplane Failure        03:42:29 UTC Apr 17 2009
Other host -   Primary
    Group 1    Active         Comm Failure             03:41:12 UTC Apr 17 2009
    Group 2    Active         Comm Failure             03:41:12 UTC Apr 17 2009
====Configuration State===
        Sync Done
====Communication State===
        Mac set
```

The following is sample output from the **show failover state** command for an active-standby setup:

```
ciscoasa(config)# show failover state
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             12:53:10 UTC Apr 26 2017
====Configuration State===
        Sync Done
```

```
====Communication State===
        Mac set
```

Table 7-2 describes the output of the **show failover state** command.

Table 50: show failover state Output Description

Field	Description
Configuration State	Displays the state of configuration synchronization. The following are possible configuration states for the standby unit: • **Config Syncing - STANDBY**—Set while the synchronized configuration is being executed. • **Interface Config Syncing - STANDBY** • **Sync Done - STANDBY**—Set when the standby unit has completed a configuration synchronization from the active unit. The following are possible configuration states for the active unit: • **Config Syncing**—Set on the active unit when it is performing a configuration synchronization to the standby unit. • **Interface Config Syncing** • **Sync Done**—Set when the active unit has completed a successful configuration synchronization to the standby unit. • **Ready for Config Sync**—Set on the active unit when the standby unit signals that it is ready to receive a configuration synchronization.
Communication State	Displays the status of the MAC address synchronization. • **Mac set**—The MAC addresses have been synchronized from the peer unit to this unit. • **Updated Mac**—Used when a MAC address is updated and needs to be synchronized to the other unit. Also used during the transition period where the unit is updating the local MAC addresses synchronized from the peer unit.
Date/Time	Displays a date and timestamp for the failure.
Last Failure Reason	Displays the reason for the last reported failure. This information is not cleared, even if the failure condition is cleared. This information changes only when a failover occurs. The following are possible fail reasons: • **Interface Failure**—The number of interfaces that failed met the failover criteria and caused failover. • **Comm Failure**—The failover link failed or peer is down. • **Backplane Failure**
State	Displays the Primary/Secondary and Active/Standby status for the unit.

Field	Description
This host/Other host	This host indicates information for the device upon which the command was executed. Other host indicates information for the other device in the failover pair.

The following is sample output from the **show failover history** command:

```
ciscoasa(config)# show failover history
==========================================================================
From State                 To State                   Reason
==========================================================================
11:59:31 UTC Jan 13 2017
Active Config Applied      Active                     No Active unit found

06:17:51 UTC Jan 15 2017
Active                     Failed                     Interface check
                                                              This Host:3
                                                                admin: inside
                                                                ctx-1: ctx1-1
                                                                ctx-2: ctx2-1
                                                              Other Host:0
03:58:49 UTC Feb 3 2017
Active                     Cold Standby               Failover state check delayed due to
 mate failure

03:58:51 UTC Feb 3 2017
Cold Standby               Sync Config                Failover state check delayed due to
 mate failure

03:59:18 UTC Feb 3 2017
Sync Config                Sync File System           Failover state check delayed due to
 mate failure
23:11:39 UTC Jan 13 2017
Cold Standby              Failed                   HA state progression failed as response
 not heard from mate

23:19:01 UTC Jan 13 2017
Sync Config                Not Detected               HA state progression failed as
configuration sync timeout expired
 14:26:28 UTC Aug 16 2017
Standby Ready              Just Active                Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Just Active                Active Drain               Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Drain               Active Applying Config     Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Applying Config     Active Config Applied      Inspection engine in other unit has
failed due to disk failure

14:26:29 UTC Aug 16 2017
Active Config Applied      Active                     Inspection engine in other unit has
failed due to disk failure

18:03:35 UTC Aug 17 2017
Active                     Standby Ready              Other unit wants me Standby
```

```
18:03:36 UTC Aug 17 2017
Standby Ready            Failed                     Detect Inspection engine failure due
 to disk failure

18:03:37 UTC Aug 17 2017
Failed                   Standby Ready              My Inspection engine is as good as
peer due to disk recovery
```

Each entry provides the time and date the state change occurred, the beginning state, the resulting state, and the reason for the state change. The newest entries are located at the bottom of the display. Older entries appear at the top. A maximum of 60 entries can be displayed. Once the maximum number of entries has been reached, the oldest entries are removed from the top of the output as new entries are added to the bottom.

The failure reasons include details that help in troubleshooting. These include interface check, failover state check, state progression failure and service module failure.

The following is sample output from the show failover history details command:

```
show failover history details
==========================================================================
From State                 To State                   Reason
==========================================================================
09:58:07 UTC Jan 18 2017
Not Detected               Negotiation                No Error
09:58:10 UTC Jan 18 2017
Negotiation                Just Active                No Active unit found
09:58:10 UTC Jan 18 2017
Just Active                Active Drain               No Active unit found
09:58:10 UTC Jan 18 2017
Active Drain               Active Applying Config     No Active unit found
09:58:10 UTC Jan 18 2017
Active Applying Config    Active Config Applied       No Active unit found
09:58:10 UTC Jan 18 2017
Active Config Applied     Active                      No Active unit found
==========================================================================
PEER History Collected at 09:58:54 UTC Jan 18 2017
=======================PEER-HISTORY=========================================
From State                To State                    Reason
=========================PEER-HISTORY=======================================
09:57:46 UTC Jan 18 2017
Not Detected              Negotiation                 No Error
09:58:19 UTC Jan 18 2017
Negotiation               Cold Standby                Detected an Active mate
09:58:21 UTC Jan 18 2017
Cold Standby             Sync Config                  Detected an Active mate
09:58:29 UTC Jan 18 2017
Sync Config             Sync File System              Detected an Active mate
09:58:29 UTC Jan 18 2017
Sync File System        Bulk Sync                     Detected an Active mate
09:58:42 UTC Jan 18 2017
Bulk Sync               Standby Ready                 Detected an Active mate
=========================PEER-HISTORY=====================================
```

The show failover history details command requests the peer's failover history and prints the unit failover history along with the peer's latest failover history. If the peer does not respond within one second it displays the last collected failover history information.

Table 7-3 shows the failover states. There are two types of states—stable and transient. Stable states are states that the unit can remain in until some occurrence, such as a failure, causes a state change. A transient state is a state that the unit passes through while reaching a stable state.

Table 51: Failover States

States	Description
Disabled	Failover is disabled. This is a stable state.
Failed	The unit is in the failed state. This is a stable state.
Negotiation	The unit establishes the connection with peer and negotiates with peer to determine software version compatibility and Active/Standby role. Depending upon the role that is negotiated, the unit will go through the Standby Unit States or the Active Unit States or enter the failed state. This is a transient state.
Not Detected	The ASA cannot detect the presence of a peer. This can happen when the ASA boots up with failover enabled but the peer is not present or is powered down.
Standby Unit States	
Cold Standby	The unit waits for the peer to reach the Active state. When the peer unit reaches the Active state, this unit progresses to the Standby Config state. This is a transient state.
Sync Config	The unit requests the running configuration from the peer unit. If an error occurs during the configuration synchronization, the unit returns to the Initialization state. This is a transient state.
Sync File System	The unit synchronizes the file system with the peer unit. This is a transient state.
Bulk Sync	The unit receives state information from the peer. This state only occurs when Stateful Failover is enabled. This is a transient state.
Standby Ready	The unit is ready to take over if the active unit fails. This is a stable state.
Active Unit States	
Just Active	The first state the unit enters when becoming the active unit. During this state a message is sent to the peer alerting the peer that the unit is becoming active and the IP and MAC addresses are set for the interfaces. This is a transient state.
Active Drain	Queues messages from the peer are discarded. This is a transient state.
Active Applying Config	The unit is applying the system configuration. This is a transient state.
Active Config Applied	The unit has finished applying the system configuration. This is a transient state.
Active	The unit is active and processing traffic. This is a stable state.

Each state change is followed by a reason for the state change. The reason typically remains the same as the unit progresses through the transient states to the stable state. The following are the possible state change reasons:

- No Error
- Set by the CI config cmd
- Failover state check

- Failover interface become OK
- HELLO not heard from mate
- Other unit has different software version
- Other unit operating mode is different
- Other unit license is different
- Other unit chassis configuration is different
- Other unit card configuration is different
- Other unit want me Active
- Other unit want me Standby
- Other unit reports that I am failed
- Other unit reports that it is failed
- Configuration mismatch
- Detected an Active mate
- No Active unit found
- Configuration synchronization done
- Recovered from communication failure
- Other unit has different set of vlans configured
- Unable to verify vlan configuration
- Incomplete configuration synchronization
- Configuration synchronization failed
- Interface check
- My communication failed
- ACK not received for failover message
- Other unit got stuck in learn state after sync
- No power detected from peer
- No failover cable
- HA state progression failed
- Detect service card failure
- Service card in other unit has failed
- My service card is as good as peer
- LAN Interface become un-configured
- Peer unit just reloaded

- Switch from Serial Cable to LAN-Based fover
- Unable to verify state of config sync
- Auto-update request
- Unknown reason

The following is sample output from the **show failover interface** command. The device has an IPv6 address configured on the failover interface.

```
ciscoasa(config)# show failover interface
        interface folink GigabitEthernet0/2
                System IP Address: 2001:a0a:b00::a0a:b70/64
                My IP Address    : 2001:a0a:b00::a0a:b70
                Other IP Address : 2001:a0a:b00::a0a:b71
```

The following is sample failover warnings output from the **show failover trace** command:

```
ciscoasa(config)# show failover trace warning
        Warning:Output can be huge. Displaying in pager mode
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer has  1  down ifcs
        Oct 14 UTC 20:56:56.345 [CABLE]    [ERROR]fover: peer rcvd down ifcs info
```

The following is sample failover output from the **show failover statistics** command for Version prior to 9.18:

```
ciscoasa(config)# show failover statistics
        tx:121456
        rx:121306
```

The following is sample failover output from the **show failover statistics** command for Version 9.18 or later:

```
ciscoasa(config)# show failover statistics
        tx:3396
        rx:3296

        Unknown version count for Fover ctl client: 0
        Unknown reason count for peer's switch reason: 0
        fover cd log create failed: 0
```

The tx and rx counters includes all the **Failover control packets**, which are sent or received over the failover LAN interface.

The "Unknown version count for Fover ctl client" counter is incremented when the **Failover control packets** has version as 0 in the received packets.

The "Unknown reason count for peer's switch reason" counter is incremented if **the received HA switchover reason from peer unit is out of locally known reason list**.

The “fover cd log create failed” is set to 1 if the fover cd log file handle was not created.

The following is sample failover output from the **show failover statistics all** command:

```
ciscoasa(config)# show failover statistics all
```

```
show failover statistics unit
-----------------------------
Unit Poll frequency 2 seconds, holdtime 10 seconds
Failover unit health statistics set size 10
1 Hold Interval Success: 3 Failure: 0
2 Hold Interval Success: 5 Failure: 0
3 Hold Interval Success: 5 Failure: 0
4 Hold Interval Success: 5 Failure: 0
5 Hold Interval Success: 5 Failure: 0

show failover statistics interface all
--------------------------------------
Interface Poll frequency 2 seconds, holdtime 10 seconds
Interface Policy 1
Monitored Interfaces 3 of 1285 maximum
Health statistics monitored interfaces 3
Failover interface health statistics set size 10
Interface: outside
 1 Hold Success: 0 Failure: 0
 2 Hold Success: 0 Failure: 0
 3 Hold Success: 0 Failure: 0
 4 Hold Success: 0 Failure: 0
 5 Hold Success: 0 Failure: 0
Interface: inside
 1 Hold Success: 0 Failure: 0
 2 Hold Success: 0 Failure: 0
 3 Hold Success: 0 Failure: 0
 4 Hold Success: 0 Failure: 0
 5 Hold Success: 0 Failure: 0
Interface: diagnostic
 1 Hold Success: 0 Failure: 0
 2 Hold Success: 0 Failure: 0
 3 Hold Success: 0 Failure: 0
 4 Hold Success: 0 Failure: 0
 5 Hold Success: 0 Failure: 0

show failover statistics np-clients
-----------------------------------

Abbreviations:
BLErr - Buffer lock error, HIErr - HA Interface error, PI - Peer incompatible
PSErr - Packet size error, IPkt - Invalid pkt, CPkt - Corrupted pkt
BErr - Buffer error, MDErr - Msg descriptor error, MxBErr - Multiplexer buffer error
MxBDErr - Multiplexer buffer descriptor error

HA DP Clients Statistics

TX Statistics
------------------------------------------------------------------------------------------
Client Name                                     Tx In        Tx Out       BLErr        HIErr
        PI
------------------------------------------------------------------------------------------
SNP HA private client                               0            0            0            0
            0
Soft NP flow stateful failover                      0            0            0            0
            0
Soft NP SVC stateful failover                       0            0            0            0
            0
SIP inspection engine                               0            0            0            0
            0
SCTP inspection engine                              0            0            0            0
            0
Soft NP NLP HA client                              16           16            0            0
```

```
            0
ODNS inspection engine                            0            0            0            0
            0
DNS BRANCH/SNOOPING module                        0            0            0            0
            0
ARP DP module                                     0            0            0            0
            0
TFW DP module                                     0            0            0            0
            0
SNP HA Heartbeat client                           1130         1130         0            0
            0
ZTNA DP module                                    0            0            0            0
            0
Unknown client                                    0            0            0            0
            0

RX Statistics
------------------------------------------------------------------------------------------
Client Name                                       Rx In        Rx Out       PSErr
IPkt         CPkt         PI
------------------------------------------------------------------------------------------
SNP HA private client                               0            0            0
 0            0            0
Soft NP flow stateful failover                      0            0            0
 0            0            0
Soft NP SVC stateful failover                       0            0            0
 0            0            0
SIP inspection engine                               0            0            0
 0            0            0
SCTP inspection engine                              0            0            0
 0            0            0
Soft NP NLP HA client                               1            1            0
 0            0            0
ODNS inspection engine                              0            0            0
 0            0            0
DNS BRANCH/SNOOPING module                          0            0            0
 0            0            0
ARP DP module                                       0            0            0
 0            0            0
TFW DP module                                       0            0            0
 0            0            0
SNP HA Heartbeat client                             1121         1121         0
 0            0            0
ZTNA DP module                                      0            0            0
 0            0            0
Unknown client                                      0            0            0
 0            0            0

Buffer Failure Statistics
------------------------------------------------------------------------------------------
Client Name                                     BErr         MDErr        MxBErr
MxBDErr
------------------------------------------------------------------------------------------
SNP HA private client                            0            0            0            0

Soft NP flow stateful failover                   0            0            0            0

Soft NP SVC stateful failover                    0            0            0            0

SIP inspection engine                            0            0            0            0

SCTP inspection engine                           0            0            0            0

Soft NP NLP HA client                            0            0            0            0
```

```
ODNS inspection engine                          0            0            0            0

DNS BRANCH/SNOOPING module                      0            0            0            0

ARP DP module                                   0            0            0            0

TFW DP module                                   0            0            0            0

SNP HA Heartbeat client                         0            0            0            0

ZTNA DP module                                  0            0            0            0

Unknown client                                  0            0            0            0

------------------------------------------------------------------------------------------

show failover statistics bulk-sync
-----------------------------------

For session 0, NP Client Bulk Sync stats
==========================================================================================

 Client Name                         Status              Start Time                  End
Time          Time Taken
==========================================================================================

 Soft NP flow stateful failover       Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 Soft NP SVC stateful failover        Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 SCTP inspection engine               Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 DNS BRANCH/SNOOPING module           Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 ARP DP module                        Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 TFW DP module                        Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
 ZTNA DP module                       Done         06:44:50 UTC Feb 10 2023   06:44:50 UTC
 Feb 10 2023   00:00:00
==========================================================================================


For session 0, CP Client Bulk Sync stats
==========================================================================================

 Client Name                                    Status               Start Time
        End Time          Time Taken
==========================================================================================

 HA Internal Control                             Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Failover Control Module                         Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Legacy LU support                               Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 vpnfo                                           Done         06:44:50 UTC Feb 10 2023
06:45:00 UTC Feb 10 2023   00:00:10
 vpnfo                                           Done         06:44:50 UTC Feb 10 2023
06:45:00 UTC Feb 10 2023   00:00:10
 SIP inspection engine                           Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
```

```
 NetFlow Module                                   Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 HA Shared License Client                         Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Route HA engine                                  Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 CTS                                              Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 CTS SXP Module                                   Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 IPv6 Route HA engine                             Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Service Tag Switching Module                     Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 CFG_HIST HA Client                               Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 SCTP inspection engine                           Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 KCD                                              Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 HA CD Proxy Client                               Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 DHCPv6 HA engine                                 Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Attribute Module                                 Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 ODNS inspection engine                           Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Ruld ID DB Client                                Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 DNS branch HA CP client                          Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 DNS_TRUSTED_SOURCE module                        Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 Threat-Detection                                 Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
 ZTNA HA Module                                   Done         06:44:50 UTC Feb 10 2023
06:44:50 UTC Feb 10 2023   00:00:00
```

The following is a sample output (only non-zero rows) from the **show failover statistics cp-clients** command:

```
show failover statistics cp-clients

Abbreviations:
TxIn - Pkt rcvd at HA from client, TxOut - Pkt sent from HA to Interface
BErr - Buffer alloc failure, MDErr - Msg desc alloc failure, AckRcvd - Ack rcvd
ReTx - Retransmit pkts, NoSvc - HA service is down, PIErr - Client is incompatible
EncErr - Error in encrypting pkt, RepCfg - Replace cfg enabled
RxIn - Pkt rcvd from Interface to HA, RxOut - Pkt sent from HA to client
MDErr - Msg desc alloc failure, AckSent - Ack sent, NMsgCb - No Msg callback for client
InVcid - Invalid vcid rcvd, PIErr - Client is incompatible, InvPkt - Invalid pkt rcvd,

HA CP Clients Statistics

TX Statistics
-----------------------------------------------------------------------------------------
Client Name                    TxIn          TxOut       BErr   MDErr  AckRcvd       ReTx
  NoSvc  PIErr  EncErr RepCfg
-----------------------------------------------------------------------------------------
Legacy LU Support  478  478 0 0 0  0 0 0 0 0
vpnfo    2  2   0 0 2  0 0 0 0 0
HA CD Proxy Client  17  17  0 0 17       0 0 0 0 0
```

```
------------------------------------------------------------------------------------------
Total Aggressive Ack rcvd      :   0

RX Statistics
------------------------------------------------------------------------------------------
Client Name                    RxIn          RxOut         MDErr  AckSent       NMsgCb
InVcid PIErr  InvPkt
------------------------------------------------------------------------------------------
Legacy LU Support  478  478  0 0  0 0 0 0
vpnfo        1960     1960   0 12  0 0 0 0
CTS    1  1      0 1  0 0 0 0
CFG_HIST HA Client  12  12   0 12  0 0 0 0
HA CD Proxy Client  10  10   0 10  0 0 0 0
ZTNA HA Module      1   1    0 1   0 0 0 0
------------------------------------------------------------------------------------------
Total Aggressive Ack sent        :   0
Total Invalid pkts rcvd          :   0
Total unknown client pkts rcvd   :   0
```

The following is a sample output (only non-zero rows) from the **show failover statistics np-clients** command:

```
show failover statistics np-clients

Abbreviations:
BLErr - Buffer lock error, HIErr - HA Interface error, PI - Peer incompatible
PSErr - Packet size error, IPkt - Invalid pkt, CPkt - Corrupted pkt
BErr - Buffer error, MDErr - Msg descriptor error, MxBErr - Multiplexer buffer error
MxBDErr - Multiplexer buffer descriptor error

HA DP Clients Statistics

TX Statistics
------------------------------------------------------------------------------------------
Client Name                     Tx In          Tx Out       BLErr   HIErr  PI
------------------------------------------------------------------------------------------
Soft NP flow stateful failover 1420091  1420091 0 0 0
Soft NP NLP HA client    45131    45131   0 0 0
Soft NP NLP HA client current  45129    45129   0 0 0
SNP HA Heartbeat Client  4240     4240    0 0 0
------------------------------------------------------------------------------------------

RX Statistics
------------------------------------------------------------------------------------------
Client Name                     Rx In          Rx Out       PSErr   IPkt  CPkt PI
------------------------------------------------------------------------------------------
Soft NP NLP HA client    7943     7943    0 0 0  0
Soft NP NLP HA client current  7943     7943    0 0 0  0
SNP HA Heartbeat client  4185     4185    0 0 0  0
------------------------------------------------------------------------------------------
Buffer Failure Statistics
------------------------------------------------------------------------------------------
Client Name                     BErr          MDErr       MxBErr MxBDErr
------------------------------------------------------------------------------------------
```

Soft NP NLP HA is the HA client.

Soft NP NLP HA Current shows the counters for app sync in the current session:

- NP = Data plane
- Soft NP = Internal constructs of the data plane
- NLP = Non-Lina processes

The following is a sample output from the **show failover statistics events** command that shows the failover events statistics information:

```
show failover statistics events

Info: Failover Lan interface came UP at 05:01:23 UTC Oct 18 2023
Codes: A -Blade Id, B -Chassis Id C -Re enable failover
===================================================================
MIO Events Table|                Time              A| B | C|
MIO heartbeat recovered| 05:00:52 UTC Oct 18 2023| 1| 0| true|
MIO heartbeat recovered| 05:04:02 UTC Oct 18 2023| 1| 0|false|
```

Related Commands

Command	Description
show running-config failover	Displays the **failover** commands in the current configuration.

show failover descriptor

Shows failover interface descriptors. It shows two numbers for every interface. When exchanging information about an interface, this unit uses the first number in the messages it sends to its peer. And it expects the second number in the messages it receives from its peer. For troubleshooting, collect the show output from both the units, and verify whether the numbers match.

show failover descriptor

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.2	This command was added.

Examples

The following is sample output from the show failover descriptor command.

```
asa# show failover descriptor
outside send:   20100ffff0001  receive:   20100ffff0002
mgmt    send:   10000ffff0001  receive:   10000ffff0002
inside  send: 20001fffff0001  receive: 20001fffff0002
```

show failover exec

To display the **failover exec** command mode for the specified unit, use the **show failover exec** command in privileged EXEC mode.

show failover exec { **active** | **standby** | **mate** }

Syntax Description

active	Displays the **failover exec** command mode for the active unit.
mate	Displays the **failover exec** command mode for the peer unit.
standby	Displays the **failover exec** command mode for the standby unit.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **failover exec** command creates a session with the specified device. By default, that session is in global configuration mode. You can change the command mode of that session by sending the appropriate command (such as the **interface** command) using the **failover exec** command. Changing **failover exec** command modes for the specified device does not change the command mode for the session you are using to access the device. Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command.

The **show failover exec** command displays the command mode on the specified device in which commands sent with the **failover exec** command are executed.

Examples

The following is sample output from the **show failover exec** command. This example demonstrates that the command mode for the unit where the **failover exec** commands are being entered does not have to be the same as the **failover exec** command mode where the commands are being executed.

In this example, an administrator logged into the standby unit adds a name to an interface on the active unit. The second time the **show failover exec mate** command is entered in this example shows the peer device in interface configuration mode. Commands sent to the device with the **failover exec** command are executed in that mode.

```
ciscoasa(config)# show failover exec mate
Active unit Failover EXEC is at config mode! The following command changes the standby unit
 failover exec mode ! to interface configuration mode.ciscoasa(config)# failover exec mate
 interface GigabitEthernet0/1
ciscoasa(config)# show failover exec mate
Active unit Failover EXEC is at interface sub-command mode! Because the following command
is sent to the active unit, it is replicated ! back to the standby unit.ciscoasa(config)#
failover exec mate nameif test
```

Related Commands

Command	Description
failover exec	Executes the supplied command on the designated unit in a failover pair.

show failover config-sync

To display details of the config-sync optimization feature, use the **show failover config-sync** command in privileged EXEC mode.

show failover config-sync { **checksum** | **configuration** | **status** }

Syntax Description

checksum	Displays the device status and checksum information.
configuration	Displays the device failover configuration and checksum information.
status	Displays the config-sync optimization status information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.18.(1)	This command was added.

Usage Guidelines

The **showfailover config-sync** command displays the status of Config Sync Optimization feature, device configuration, and the checksum information. By default, that session is in global configuration mode.

Examples

The following are the sample output from the **showfailoverconfig-syncchecksum** command for the active and standby units.

```
ciscoasa# show failover config-sync checksum
My State: Active
Config Hash: 12daf457c6a1e875a175a67cab7f0c56
```

```
ciscoasa# show failover config-sync checksum
My State: Standby Ready
Config Hash: 12daf457c6a1e875a175a67cab7f0c56
```

The following are the sample output from the **showfailoverconfig-syncconfiguration** command.

```
cicoasa#show failover config-sync configuration
My State: Negotiation
[1]: Cmd_: !
[2]: Cmd_: enable password $sha512$5000$eTI8yiQxuWYEzeypFF6qdw==$HNf7i1tpOugBBnUSIzrlPA==
pbkdf2
[3]: Cmd_: service-module 0 keepalive-timeout 4
[4]: Cmd_: service-module 0 keepalive-counter 6
[5]: Cmd_: !
[6]: Cmd_: license smart
[7]: Cmd_:  feature tier standard
[8]: Cmd_:  throughput level 10G
[9]: Cmd_: names
[10]: Cmd_: no mac-address auto
[11]: Cmd_: !
[12]: Cmd_: interface GigabitEthernet0/0
[13]: Cmd_:  shutdown
[14]: Cmd_:  no nameif
[15]: Cmd_:  no security-level
[16]: Cmd_:  no ip address
[17]: Cmd_: !
[18]: Cmd_: interface GigabitEthernet0/1
[19]: Cmd_:  shutdown
[20]: Cmd_:  no nameif
[21]: Cmd_:  no security-level
[22]: Cmd_:  no ip address
[23]: Cmd_: !
[24]: Cmd_: interface GigabitEthernet0/2
[25]: Cmd_:  shutdown
[26]: Cmd_:  no nameif
[27]: Cmd_:  no security-level
[28]: Cmd_:  no ip address
[29]: Cmd_: !
[30]: Cmd_: interface GigabitEthernet0/3
[31]: Cmd_:  shutdown
[32]: Cmd_:  no nameif
[33]: Cmd_:  no security-level
[34]: Cmd_:  no ip address
[35]: Cmd_: !
[36]: Cmd_: interface GigabitEthernet0/4
[37]: Cmd_:  shutdown
[38]: Cmd_:  no nameif
[39]: Cmd_:  no security-level
[40]: Cmd_:  no ip address
[41]: Cmd_: !
[42]: Cmd_: interface GigabitEthernet0/5
[43]: Cmd_:  shutdown
[44]: Cmd_:  no nameif
[45]: Cmd_:  no security-level
[46]: Cmd_:  no ip address
[47]: Cmd_: !
[48]: Cmd_: interface GigabitEthernet0/6
[49]: Cmd_:  shutdown
[50]: Cmd_:  no nameif
[51]: Cmd_:  no security-level
[52]: Cmd_:  no ip address
[53]: Cmd_: !
[54]: Cmd_: interface GigabitEthernet0/7
[55]: Cmd_:  shutdown
[56]: Cmd_:  no nameif
[57]: Cmd_:  no security-level
[58]: Cmd_:  no ip address
[59]: Cmd_: !
[60]: Cmd_: interface GigabitEthernet0/8
```

```
[61]: Cmd_:  description LAN/STATE Failover Interface
[62]: Cmd_: !
[63]: Cmd_: interface Management0/0
[64]: Cmd_:  no management-only
[65]: Cmd_:  nameif management
[66]: Cmd_:  security-level 0
[67]: Cmd_:  ip address 192.168.2.63 255.255.255.0 standby 192.168.2.64
[68]: Cmd_: !
[69]: Cmd_: ftp mode passive
[70]: Cmd_: no object-group-search access-control
[71]: Cmd_: pager lines 23
[72]: Cmd_: mtu management 1500
[73]: Cmd_: failover
[74]: Cmd_: failover lan interface fover GigabitEthernet0/8
[75]: Cmd_: failover link fover GigabitEthernet0/8
[76]: Cmd_: failover interface ip fover 10.0.0.63 255.255.255.0 standby 10.0.0.64
[77]: Cmd_: no failover wait-disable
[78]: Cmd_: no monitor-interface service-module
[79]: Cmd_: icmp unreachable rate-limit 1 burst-size 1
[80]: Cmd_: no asdm history enable
[81]: Cmd_: arp timeout 14400
[82]: Cmd_: no arp permit-nonconnected
[83]: Cmd_: arp rate-limit 32768
[84]: Cmd_: route management 0.0.0.0 0.0.0.0 192.168.2.1 1
[85]: Cmd_: timeout xlate 3:00:00
[86]: Cmd_: timeout pat-xlate 0:00:30
[87]: Cmd_: timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02
[88]: Cmd_: timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
[89]: Cmd_: timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
[90]: Cmd_: timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
[91]: Cmd_: timeout tcp-proxy-reassembly 0:01:00
[92]: Cmd_: timeout floating-conn 0:00:00
[93]: Cmd_: timeout conn-holddown 0:00:15
[94]: Cmd_: timeout igp stale-route 0:01:10
[95]: Cmd_: user-identity default-domain LOCAL
[96]: Cmd_: aaa authentication ssh console LOCAL
[97]: Cmd_: aaa authentication login-history
[98]: Cmd_: http server enable
[99]: Cmd_: http 0.0.0.0 0.0.0.0 management
[100]: Cmd_: no snmp-server location
[101]: Cmd_: no snmp-server contact
[102]: Cmd_: crypto ipsec security-association pmtu-aging infinite
[103]: Cmd_: crypto ca trustpoint _SmartCallHome_ServerCA
[104]: Cmd_:  no validation-usage
[105]: Cmd_:  crl configure
[106]: Cmd_: crypto ca trustpoint _SmartCallHome_ServerCA2
[107]: Cmd_:  no validation-usage
[108]: Cmd_:  crl configure
[109]: Cmd_: crypto ca trustpool policy
[110]: Cmd_:  auto-import
[111]: Cmd_: crypto ca certificate chain _SmartCallHome_ServerCA
[112]: Cmd_:  certificate ca 0a0142800000014523c844b500000002
[113]: Cmd_:     30820560 30820348 a0030201 0202100a 01428000 00014523 c844b500 00000230
[114]: Cmd_:     0d06092a 864886f7 0d01010b 0500304a 310b3009 06035504 06130255 53311230
[115]: Cmd_:     10060355 040a1309 4964656e 54727573 74312730 25060355 0403131e 4964656e
[116]: Cmd_:     54727573 7420436f 6d6d6572 6369616c 20526f6f 74204341 2031301e 170d3134
[117]: Cmd_:     30313136 31383132 32335a17 0d333430 31313631 38313232 335a304a 310b3009
[118]: Cmd_:     06035504 06130255 53311230 10060355 040a1309 4964656e 54727573 74312730
[119]: Cmd_:     25060355 0403131e 4964656e 54727573 7420436f 6d6d6572 6369616c 20526f6f
[120]: Cmd_:     74204341 20313082 0222300d 06092a86 4886f70d 01010105 00038202 0f003082
[121]: Cmd_:     020a0282 020100a7 5019de3f 993dd433 46f16f51 6182b2a9 4f8f6789 5d84d953
[122]: Cmd_:     dd0c28d9 d7f0ffae 95437299 f9b55d7c 8ac142e1 315074d1 810d7ccd 9b21ab43
[123]: Cmd_:     e2acad5e 866ef309 8a1f5a32 bda2eb94 f9e85c0a ecff98d2 af71b3b4 539f4e87
[124]: Cmd_:     ef92bcbd ec4f3230 884b175e 57c453c2 f602978d d9622bbf 241f628d dfc3b829
```

```
[125]: Cmd_:     4b49783c 93608822 fc99da36 c8c2a2d4 2c540067 356e73bf 0258f0a4 dde5b0a2
[126]: Cmd_:     267acae0 36a51916 f5fdb7ef ae3f40f5 6d5a04fd ce34ca24 dc74231b 5d331312
[127]: Cmd_:     5dc40125 f630dd02 5d9fe0d5 47bdb4eb 1ba1bb49 49d89f5b 02f38ae4 2490e462
[128]: Cmd_:     4f4fc1af 8b0e7417 a8d17288 6a7a0149 ccb44679 c617b1da 981e0759 fa752185
[129]: Cmd_:     65dd9056 cefbaba5 609dc49d f952b08b bd87f98f 2b230a23 763bf733 e1c900f3
[130]: Cmd_:     69f94ba2 e04ebc7e 93398407 f744707e fe075ae5 b1acd118 ccf235e5 494908ca
[131]: Cmd_:     56c93dfb 0f187d8b 3bc113c2 4d8fc94f 0e37e91f a10e6adf 622ecb35 0651792c
[132]: Cmd_:     c82538f4 fa4ba789 5c9cd2e3 0d39864a 747cd559 87c23f4e 0c5c52f4 3df75282
[133]: Cmd_:     f1eaa3ac fd49341a 28f34188 3a13eee8 deff991d 5fbacbe8 1ef2b950 60c031d3
[134]: Cmd_:     73e5efbe a0ed330b 74be2020 c4676cf0 08037a55 807f464e 96a7f41e 3ee1f6d8
[135]: Cmd_:     09e13364 2b63d732 5e9ff9c0 7b0f786f 97bc939a f99c1290 787a8087 15d77274
[136]: Cmd_:     9c557478 b1bae16e 7004ba4f a0ba68c3 7bff31f0 733d3d94 2ab10b41 0ea0fe4d
[137]: Cmd_:     88656b79 33b4d702 03010001 a3423040 300e0603 551d0f01 01ff0404 03020106
[138]: Cmd_:     300f0603 551d1301 01ff0405 30030101 ff301d06 03551d0e 04160414 ed4419c0
[139]: Cmd_:     d3f0068b eea47bbe 42e72654 c88e3676 300d0609 2a864886 f70d0101 0b050003
[140]: Cmd_:     82020100 0dae9032 f6a64b7c 44761961 1e2728cd 5e54ef25 bce30890 f929d7ae
[141]: Cmd_:     6808e194 0058ef2e 2e7e5352 8cb65c07 ea88ba99 8b5094d7 8280df61 090093ad
[142]: Cmd_:     0d14e6ce c1f23794 78b05f9c b3a273b8 8f059338 cd8d3eb0 b8fbc0cf b1f2ec2d
[143]: Cmd_:     2d1bccec aa9ab3aa 60821b2d 3bc3843d 578a961e 9c75b8d3 30cd6008 8390d38e
[144]: Cmd_:     54f14d66 c05d7403 40a3ee85 7ec21f77 9c06e8c1 a7185d52 95edc9dd 259e6dfa
[145]: Cmd_:     a9eda33a 34d0597b daed50f3 35bfedeb 144d31c7 60f4daf1 879ce248 e2c6c537
[146]: Cmd_:     fb0610fa 75596631 4729da76 9a1ce982 aeef9ab9 51f78823 9a699562 3ce55580
[147]: Cmd_:     36d75402 fff1b95d ced4236f d845844a 5b65ef89 0cdd14a7 20cb18a5 25b40df9
[148]: Cmd_:     01f0a2d2 f400c874 8ea12a48 8e65db13 c4e22517 7debbe87 5b172054 51934a53
[149]: Cmd_:     030bec5d ca33ed62 fd45c72f 5bdc58a0 8039e6fa d7fe1314 a6ed3d94 4a4274d4
[150]: Cmd_:     c3775973 cd8f46be 5538effa e89132ea 97580422 de38c3cc bc6dc933 3a6a0a69
[151]: Cmd_:     3fa0c8ea 728f8c63 8623bd6d 3c969e95 e0494caa a2b92a1b 9c368178 edc3e846
[152]: Cmd_:     e2265944 751ed975 8951cd10 849d6160 cb5df997 224d8e98 e6e37ff6 5bbbaecd
[153]: Cmd_:     ca4a816b 5e0bf351 e1742be9 7e27a7d9 99494ef8 a580db25 0f1c6362 8ac93367
[154]: Cmd_:     6b3c1083 c6addea8 cd168e8d f0073771 9ff2abfc 41f5c18b ec00375d 09e54e80
[155]: Cmd_:     effab15c 3806a51b 4ae1dc38 2d3cdcab 1f901ad5 4a9ceed1 706cccee f457f818
[156]: Cmd_:     ba846e87
[157]: Cmd_:   quit
[158]: Cmd_: crypto ca certificate chain _SmartCallHome_ServerCA2
[159]: Cmd_:  certificate ca 0509
[160]: Cmd_:     308205b7 3082039f a0030201 02020205 09300d06 092a8648 86f70d01 01050500
[161]: Cmd_:     3045310b 30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164
[162]: Cmd_:     6973204c 696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f
[163]: Cmd_:     6f742043 41203230 1e170d30 36313132 34313832 3730305a 170d3331 31313234
[164]: Cmd_:     31383233 33335a30 45310b30 09060355 04061302 424d3119 30170603 55040a13
[165]: Cmd_:     1051756f 56616469 73204c69 6d697465 64311b30 19060355 04031312 51756f56
[166]: Cmd_:     61646973 20526f6f 74204341 20323082 0222300d 06092a86 4886f70d 01010105
[167]: Cmd_:     00038202 0f003082 020a0282 0201009a 18ca4b94 0d002daf 03298af0 0f81c8ae
[168]: Cmd_:     4c19851d 089fab29 4485f32f 81ad321e 9046bfa3 86261a1e fe7e1c18 3a5c9c60
[169]: Cmd_:     172a3a74 8333307d 615411cb edabe0e6 d2a27ef5 6b6f18b7 0a0b2dfd e93eef0a
[170]: Cmd_:     c6b310e9 dcc24617 f85dfda4 daff9e49 5a9ce633 e62496f7 3fba5b2b 1c7a35c2
[171]: Cmd_:     d667feab 66508b6d 28602bef d760c3c7 93bc8d36 91f37ff8 db1113c4 9c7776c1
[172]: Cmd_:     aeb7026a 817aa945 83e205e6 b956c194 378f4871 6322ec17 6507958a 4bdf8fc6
[173]: Cmd_:     5a0ae5b0 e35f5e6b 11ab0cf9 85eb44e9 f80473f2 e9fe5c98 8cf573af 6bb47ecd
[174]: Cmd_:     d45c022b 4c39e1b2 95952d42 87d7d5b3 9043b76c 13f1dedd f6c4f889 3fd175f5
[175]: Cmd_:     92c391d5 8a88d090 ecdc6dde 89c26571 968b0d03 fd9cbf5b 16ac92db eafe797c
[176]: Cmd_:     adebaff7 16cbdbcd 252be51f fb9a9fe2 51cc3a53 0c48e60e bdc9b476 0652e611
[177]: Cmd_:     13857263 0304e004 362b2019 02e874a7 1fb6c956 66f07525 dc67c10e 616088b3
[178]: Cmd_:     3ed1a8fc a3da1db0 d1b12354 df44766d ed41d8c1 b222b653 1cdf351d dca1772a
[179]: Cmd_:     31e42df5 e5e5dbc8 e0ffe580 d70b63a0 ff33a10f ba2c1515 ea97b3d2 a2b5bef2
[180]: Cmd_:     8c961e1a 8f1d6ca4 6137b986 7333d797 969e237d 82a44c81 e2a1d1ba 675f9507
[181]: Cmd_:     a32711ee 16107bbc 454a4cb2 04d2abef d5fd0c51 ce506a08 31f991da 0c8f645c
[182]: Cmd_:     03c33a8b 203f6e8d 673d3ad6 fe7d5b88 c95efbcc 61dc8b33 77d34432 35096204
[183]: Cmd_:     921610d8 9e2747fb 3b21e3f8 eb1d5b02 03010001 a381b030 81ad300f 0603551d
[184]: Cmd_:     130101ff 04053003 0101ff30 0b060355 1d0f0404 03020106 301d0603 551d0e04
[185]: Cmd_:     1604141a 8462bc48 4c332504 d4eed0f6 03c41946 d1946b30 6e060355 1d230467
[186]: Cmd_:     30658014 1a8462bc 484c3325 04d4eed0 f603c419 46d1946b a149a447 3045310b
[187]: Cmd_:     30090603 55040613 02424d31 19301706 0355040a 13105175 6f566164 6973204c
[188]: Cmd_:     696d6974 6564311b 30190603 55040313 1251756f 56616469 7320526f 6f742043
```

```
[189]: Cmd_:     41203282 02050930 0d06092a 864886f7 0d010105 05000382 0201003e 0a164d9f
[190]: Cmd_:     065ba8ae 715d2f05 2f67e613 4583c436 f6f3c026 0c0db547 645df8b4 72c946a5
[191]: Cmd_:     03182755 89787d76 ea963480 1720dce7 83f88dfc 07b8da5f 4d2e67b2 84fdd944
[192]: Cmd_:     fc775081 e67cb4c9 0d0b7253 f8760707 4147960c fbe08226 93558cfe 221f6065
[193]: Cmd_:     7c5fe726 b3f73290 9850d437 7155f692 2178f795 79faf82d 26876656 3077a637
[194]: Cmd_:     78335210 58ae3f61 8ef26ab1 ef187e4a 5963ca8d a256d5a7 2fbc561f cf39c1e2
[195]: Cmd_:     fb0aa815 2c7d4d7a 63c66c97 443cd26f c34a170a f890d257 a21951a5 2d9741da
[196]: Cmd_:     074fa950 da908d94 46e13ef0 94fd1000 38f53be8 40e1b46e 561a20cc 6f588ded
[197]: Cmd_:     2e458fd6 e9933fe7 b12cdf3a d6228cdc 84bb226f d0f8e4c6 39e90488 3cc3baeb
[198]: Cmd_:     557a6d80 9924f56c 01fbf897 b0945beb fdd26ff1 77680d35 6423acb8 55a103d1
[199]: Cmd_:     4d4219dc f8755956 a3f9a849 79f8af0e b911a07c b76aed34 d0b62662 381a870c
[200]: Cmd_:     f8e8fd2e d3907f07 912a1dd6 7e5c8583 99b03808 3fe95ef9 3507e4c9 626e577f
[201]: Cmd_:     a75095f7 bac89be6 8ea201c5 d666bf79 61f33c1c e1b9825c 5da0c3e9 d848bd19
[202]: Cmd_:     a2111419 6eb2861b 683e4837 1a88b75d 965e9cc7 ef276208 e291195c d2f121dd
[203]: Cmd_:     ba174282 97718153 31a99ff6 7d62bf72 e1a3931d cc8a265a 0938d0ce d70d8016
[204]: Cmd_:     b478a53a 874c8d8a a5d54697 f22c10b9 bc5422c0 01506943 9ef4b2ef 6df8ecda
[205]: Cmd_:     f1e3b1ef df918f54 2a0b25c1 2619c452 100565d5 8210eac2 31cd2e
[206]: Cmd_:   quit
[207]: Cmd_: telnet timeout 5
[208]: Cmd_: ssh stack ciscossh
[209]: Cmd_: ssh stricthostkeycheck
[210]: Cmd_: ssh timeout 5
[211]: Cmd_: ssh key-exchange group dh-group14-sha256
[212]: Cmd_: ssh 0.0.0.0 0.0.0.0 management
[213]: Cmd_: console timeout 0
[214]: Cmd_: console serial
[215]: Cmd_: threat-detection basic-threat
[216]: Cmd_: threat-detection statistics access-list
[217]: Cmd_: no threat-detection statistics tcp-intercept
[218]: Cmd_: dynamic-access-policy-record DfltAccessPolicy
[219]: Cmd_: username admin password
$sha512$5000$w9Jv9lDWNVn4XKSG1i0G6Q==$JgmsMmRSYz+ZQX3Ta/bXxA== pbkdf2 privilege 15
[220]: Cmd_: !
[221]: Cmd_: class-map inspection_default
[222]: Cmd_:  match default-inspection-traffic
[223]: Cmd_: !
[224]: Cmd_: !
[225]: Cmd_: policy-map type inspect dns preset_dns_map
[226]: Cmd_:  parameters
[227]: Cmd_:   message-length maximum client auto
[228]: Cmd_:   message-length maximum 512
[229]: Cmd_:   no tcp-inspection
[230]: Cmd_: policy-map global_policy
[231]: Cmd_:  class inspection_default
[232]: Cmd_:   inspect ip-options
[233]: Cmd_:   inspect netbios
[234]: Cmd_:   inspect rtsp
[235]: Cmd_:   inspect sunrpc
[236]: Cmd_:   inspect tftp
[237]: Cmd_:   inspect dns preset_dns_map
[238]: Cmd_:   inspect ftp
[239]: Cmd_:   inspect h323 h225
[240]: Cmd_:   inspect h323 ras
[241]: Cmd_:   inspect rsh
[242]: Cmd_:   inspect esmtp
[243]: Cmd_:   inspect sqlnet
[244]: Cmd_:   inspect sip
[245]: Cmd_:   inspect skinny
[246]: Cmd_: policy-map type inspect dns migrated_dns_map_2
[247]: Cmd_:  parameters
[248]: Cmd_:   message-length maximum client auto
[249]: Cmd_:   message-length maximum 512
[250]: Cmd_:   no tcp-inspection
[251]: Cmd_: policy-map type inspect dns migrated_dns_map_1
```

```
[252]: Cmd_:  parameters
[253]: Cmd_:   message-length maximum client auto
[254]: Cmd_:   message-length maximum 512
[255]: Cmd_:   no tcp-inspection
[256]: Cmd_: !
[257]: Cmd_: service-policy global_policy global
[258]: Cmd_: prompt hostname context
[259]: Cmd_: call-home reporting anonymous prompt 1
[260]: Cmd_: call-home
[261]: Cmd_:  profile License
[262]: Cmd_:   destination address http
https://sch-alpha.cisco.com/its/service/oddce/services/DDCEService
[263]: Cmd_:   destination transport-method http
[264]: Cmd_:  profile CiscoTAC-1
[265]: Cmd_:   no active
[266]: Cmd_:   destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
[267]: Cmd_:   destination address email callhome@cisco.com
[268]: Cmd_:   destination transport-method http
[269]: Cmd_:   subscribe-to-alert-group diagnostic
[270]: Cmd_:   subscribe-to-alert-group environment
[271]: Cmd_:   subscribe-to-alert-group inventory periodic monthly
[272]: Cmd_:   subscribe-to-alert-group configuration periodic monthly
[273]: Cmd_:   subscribe-to-alert-group telemetry periodic daily
My State: Negotiation
Config content_size: 11323
Config Hash: 9d653d6fb48739651f5467a1aebea31c
```

The following are the sample output from the **showfailoverconfig-syncstatus** command when Config Sync Optimization feature is enabled on the device.

```
ciscoasa# show failover config-sync status
Config Sync Optimization is enable
```

Related Commands

Command	Description
failover exec	Executes the supplied command on the designated unit in a failover pair.

show file

To display information about the file system, use the **show file** command in privileged EXEC mode.

show file descriptors | system | information *filename*

Syntax Description

descriptors	Displays all open file descriptors.
filename	Specifies the filename.
information	Displays information about a specific file, including partner application package files.
system	Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	The capability to view information about partner application package files was added.
9.7(1)	The **show file descriptor** command was updated to print the output, only from the open file descriptor in the system context mode.

Usage Guidelines

The **show file descriptors** command when used in System context in Multi context mode, it traverses through all the contexts and displays details of file descriptors if they are opened. If a context has an open file descriptor, only the details of that specific context is displayed, when the CLI is executed in the System context. The system does not print all the names of the context with “no file descriptors”. Only the context with open file descriptor is displayed.

Examples

The following is sample output from the **show firewall** command:

Single context with no open file

```
ciscoasa(config)# show file descriptors
```

```
No open file descriptors
ciscoasa(config)#
```

Single context with open files

```
ciscoasa(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0302  139  disk0:/test1.txt
ciscoasa(config)#
```

Multicontext with no open files in the System context

```
ciscoasa# show file descriptors
ciscoasa#
```

Multicontext with open files in the System context

```
ST-Campus-spyc/stby(config)# show file descriptors
Context: CTX1
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX3
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
Context: CTX5
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
```

Multicontext with no open files in the User context

```
ST-Campus-spyc/stby/CTX1(config)# changeto context CTX2
ST-Campus-spyc/act/CTX2(config)# show file descriptors
No open file descriptors
ST-Campus-spyc/act/CTX2(config)#
```

Multicontext with open files in the User context

```
ST-Campus-spyc/stby(config)# changeto con CTX1
ST-Campus-spyc/stby/CTX1(config)# show file descriptors
FD  Position  Open  PID  Path
0 0 0000  180  disk0:/SHARED/anyconnect-linux-3.1.07021-k9.pkg
1 0 0000  180  disk0:/SHARED/anyconnect-win-4.0.02052-k9.pkg
ST-Campus-spyc/stby/CTX1(config)#
ciscoasa# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

The following is sample output from the **show file info** command:

```
ciscoasa# show file info disk0:csc_embd1.0.1000.pkg
type is package (csc)
file size is 17204149 bytes version 1
```

Related Commands

Command	Description
dir	Displays the directory contents.
pwd	Displays the current working directory.

show fips

To show the fips status, use the **show fips** command in privileged EXEC mode.

show fips

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was added.

Usage Guidelines

The **show running-configuration fips** command displayed the status only when fips was enabled. In order to know the actual operational state, the **show fips** command was introduced. Thus, this command displays the fips status when an user enables or disables fips that is in disabled or enabled state. This command also displays status for rebooting the device after an enable or disable action.

Examples

The following are sample outputs from the **show fips** command:

When FIPS is disabled and an user enables it by running **fips enable**

```
ciscoasa# show fips
FIPS is currently disabled and will be enabled after reboot
```

After ASA is rebooted,

```
ciscoasa# show fips
FIPS is currently enabled
```

When FIPS is enabled and an user disables it by running **no fips enable**:

```
ciscoasa# show fips
FIPS is currently enabled and will be disabled after reboot
```

After ASA is rebooted,

```
ciscoasa# show fips
FIPS is currently disabled
```

When FIPS is disabled and an user disables it by running **no fips enable**

```
ciscoasa# show fips
FIPS is currently disabled
```

When FIPS is enabled and an user enables it by running **fips enable**

```
ciscoasa# show fips
FIPS is currently enabled
```

Related Commands

Command	Description
fips enable	Enables FIPS on ASA.
show running-configuration fips	Shows the current running and operational configuration of fips.

show firewall

To show the current firewall mode (routed or transparent), use the **show firewall** command in privileged EXEC mode.

show firewall

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show firewall** command:

```
ciscoasa# show firewall
Firewall mode: Router
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode.
show mode	Shows the current context mode, either single or multiple.

show flash

To display the contents of the internal Flash memory, use the **show flash:** command in privileged EXEC mode.

show flash: all | controller | filesys

Note In the ASA, the **flash** keyword is aliased to **disk0**.

Syntax Description

all	Displays all Flash information.
controller	Displays file system controller information.
filesys	Displays file system information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show flash:** command:

```
ciscoasa# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log
10170368 bytes available (52711424 bytes used)
```

Related Commands

Command	Description
dir	Displays the directory contents.
show disk0:	Displays the contents of the internal Flash memory.
show disk1:	Displays the contents of the external Flash memory card.

show flow-export counters

To display runtime counters associated with NetFlow data, use the **show flow-export counters** command in privileged EXEC mode.

show flow-export counters

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(1)	This command was added.
9.0(1)	A new error counter was added for source port allocation failure.

Usage Guidelines

The runtime counters include statistical data as well as error data.

Examples

The following is sample output from the **show flow-export counters** command, which shows runtime counters that are associated with NetFlow data:

```
ciscoasa# show flow-export counters
destination: inside 209.165.200.224 2055
 Statistics:
  packets sent                     1000
 Errors:
  block allocation failure            0
  invalid interface                   0
  template send failure               0
  no route to collector               0
  source port allocation              0
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.

show flow-offload

To display information about flow off-loading, use the **show flow-offload** command in privileged EXEC mode.

show flow-offload { **info** [**detail**] | **cpu** | **flow** [**count** | **detail**] | **statistics** }

Syntax Description

info [**detail**]	Shows basic information about the offload engine. Add the **detail** keyword to get additional information such as a summary of port usage.
cpu	Shows the load percentage on offload cores.
flow [**count** | **detail**]	Shows information on the active off-loaded flows. You can optionally add the following keywords: • **count** —Shows the number of off-loaded active flows and offloaded flows created. • **detail** —Shows the active off-loaded flows and their rewrite rules and data.
statistics	Shows the packet statistics of off-loaded flows.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was introduced.

Usage Guidelines

If you enable flow off-loading, use this command to view information about the service and the off-loaded flows.

Examples

Following is example output from the **show flow-offload flow** command. Offloaded flows are identified by an index number, which is calculated by hashing the source and destination IP addresses, ports, and the protocol. A *collision* occurs when the system tries to offload a flow that has the same index as a currently active offloaded flow. In this case, the new flow is not offloaded, but the first flow remains offloaded.

```
>show flow-offload flow
Total offloaded flow stats: 1 in use, 5 most used, 100% offloaded, 0 collisions
UDP intfc 103 src 10.1.1.2:41110 dest 20.1.1.2:5001, dynamic, timestamp 162810457, packets
 84040, bytes 127404640
```

The following is sample output from the **show flow-offload statistics** command. The output shows counts for transmitted (Tx), received (Rx) and dropped packets, and statistics for the virtual NIC (VNIC) used.

```
ciscoasa# show offload-engine statistics

Packet stats of port : 0
        Tx Packet count                 :        785807566
        Rx Packet count                 :        785807566
        Dropped Packet count            :                0
        VNIC transmitted packet         :        785807566
        VNIC transmitted bytes          :     103726598712
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
 Packet stats of port : 1
        Tx Packet count                 :                0
        Rx Packet count                 :                0
        Dropped Packet count            :                0
        VNIC transmitted packet         :                0
        VNIC transmitted bytes          :                0
        VNIC Dropped packets            :                0
        VNIC erroneous received         :                0
        VNIC CRC errors                 :                0
        VNIC transmit failed            :                0
        VNIC multicast received         :                0
```

Following is an example of information detail.

```
ciscoasa(config)# show flow-offload info detail

Current running state        : Enabled
User configured state        : Enabled
Dynamic flow offload         : Enabled
Offload App                  : Running
Offload allocated cores      : S0[ 2]
Offload Nic                  : 9
Max PKT burst                : 32
Port-0 details :
        FQ queue number      :           1440
        Keep alive counter   :         101584
flow table refresh count     : 186 [58]
HW flow table refresh count  : Port-0[58, 58, 58, 58]
Refresh count synched        : 3 times [3/0]
Flow table status Port-0     : Good
```

The refresh count information at the bottom of the output indicates the status of the flow tables kept in software (ASA) and hardware. The “refresh count” is the number of times the flow-table was invalidated, which could be due to multiple events such as route changes (addition/deletion) from software to hardware, MAC address change, and so forth.

- Flow table refresh count is the number of times the flow-table needed be invalidated. This value is maintained in ASA software.

- HW flow table refresh count is the number of times the hardware flow-table was invalidated. This value is maintained in the hardware.
- Refresh count synched is the number of times the "flow table refresh count" is explicitly synchronized from software to hardware. This happens whenever there was a mismatch between them. Normally, "flow table refresh count" and "HW flow table refresh count" will be in sync and there is no need to synchronize those values explicitly. Normally, the parameter "Refresh count synched" will be zero.
- "Flow table status" is either Good or Bad. Good indicates that "flow table refresh count" and "HW flow table refresh count" are in sync. Bad indicates a mismatch, even after trying to explicitly synchronize them. This could happen in rare condition like the CRUZ firmware is stuck or unresponsive for any update requests from the ASA software.

Related Commands

Command	Description
clear flow-offload	Clears off-load statistics or flows.
flow-offload	Enables flow off-load.
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.

show flow-offload-ipsec

To display information about IP sec flow off-loading, use the **show flow-offload-ipsec** command in privileged EXEC mode.

show flow-offload-ipsec { **info** | **option-table** | **statistics** }

Syntax Description

info	Show information about the current configuration state for IPsec flow offload.
option-table	Show table information for the content addressable memory (CAM) used in IPsec flow offload. This information is for debugging only and it is not meaningful to an end user.
statistics	Show content addressable memory (CAM) statistics for the offloaded flows.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	This command was introduced.

Example

The following example shows the current configuration state of IPsec flow offload.

```
ciscoasa# show flow-offload-ipsec info
IPSec offload : Enabled
Egress optimization: Enabled
```

The following example shows statistics.

```
ciscoasa# show flow-offload-ipsec statistics

        Packet stats of Pipe 0
        ----------------------
        Rx Packet count                                :                0
        Tx Packet count                                :                0
        Error Packet count                             :                0
        Drop Packet count                              :                0
        CAM stats of Pipe 0
        ----------------------
        Option ID Table CAM Hit Count                    :             38
        Option ID Table CAM Miss Count                   :            154
        Tunnel Table CAM Hit Count                       :              0
        Tunnel Table CAM Miss Count                      :              0
        6-Tuple CAM Hit Count                            :              0
        6-Tuple CAM Miss Count                           :             38
```

The following example shows the option table.

```
ciscoasa# show flow-offload-ipsec option-table
        instance_id:256 interface_id:124 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:123 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:122 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:121 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:120 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:119 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:118 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:117 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:156 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:157 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:158 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:159 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:112 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:111 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:110 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:109 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:108 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:107 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:106 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:105 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:104 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:103 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:102 action:0 logic_id_opt:0 subinterface_id_opt:0
        instance_id:256 interface_id:101 action:0 logic_id_opt:0 subinterface_id_opt:0
```

Related Commands

Command	Description
clear flow-offload-ipsec	Clears IPsec flow offload statistics.
flow-offload-ipsec	Configures IPsec flow offload.

show fragment

To display the operational data of the IP fragment reassembly module, enter the **show fragment** command in privileged EXEC mode.

show fragment [*interface*]

Syntax Description

interface	(Optional) Specifies the ASA interface.

Command Default

If an *interface* is not specified, the command applies to all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The command was separated into two commands, **show fragment** and **show running-config fragment**, to separate the configuration data from the operational data.
9.15(1)	The output for the **show fragment** command was enhanced to include IP fragment related drops and error counters.

Examples

This example displays the operational data of the IP fragment reassembly module:

```
ciscoasa# show fragment
Interface: inside
    Configuration: Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Run-time stats: Queue: 0, Full assembly: 12
    Drops: Size overflow: 0, Timeout: 0,
           Chain overflow: 0, Fragment queue threshold exceeded: 0,
           Small fragments: 0, Invalid IP len: 0,
           Reassembly overlap: 26595, Fraghead alloc failed: 0,
           SGT mismatch: 0, Block alloc failed: 0,
           Invalid IPV6 header: 0
```

Where:

- Size: The maximum number of blocks that are allowed to reside in fragment database (per interface) at any given point that you had configured as default.
- Chain: The maximum number of fragments into which a full IP packet can be fragmented. The default is 24.

- Timeout: The maximum number of seconds to wait for an entire fragmented packet to arrive. The default is 5 seconds.
- Reassembly: virtual or full. The default is virtual reassembly. IP fragments that terminate at the ASA or require inspection at the application level are fully (physically) reassembled. The packet that was fully (physically) reassembled can be fragmented again on the egress interface, if necessary.
- Runtime stats: Queue. The number of fragments in the reassembly database currently awaiting reassembly.
- Runtime stats: Full Assembly. The number of IP packets fully reassembled.
- Size Overflow: The maximum number of blocks that are allowed to reside in fragment database at any given point has reached. The overflow counter measures the drops due to reaching the default size for fragment data base. This counter does not include the number of fragments that are dropped because of queue size (2/3 of the max DB size).
- Timeout: The fragment chain timed out before the reassembly was completed.
- Chain limit: The individual fragment chain limit has reached.
- Fragment queue threshold exceeded: The fragment database threshold, that is 2/3 of the queue size per interface, has exceeded.
- Small fragments: When fragment offset is greater than 0 but less than 16.
- Invalid packet len: Invalid IP packet length (for example, len > 65535).
- Reassembly overlap: Duplicate or overlapping fragments were detected.
- Fraghead alloc failed: Failed to allocate fragment head. Fraghead maintains the chain of all fragments for an IP packet.
- SGT mismatch: SGT value did not match among fragments of the same IP packets.
- Block alloc failed: Allocation failed for full reassembly.
- Invalid IPV6 header: Encountered invalid IPV6 header during full reassembly.

Related Commands

Command	Description
clear configure fragment	Clears the IP fragment reassembly configuration and resets the defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
fragment	Provides additional management of packet fragmentation and improves compatibility with NFS.
show running-config fragment	Displays the IP fragment reassembly configuration.

show fxos mode

To view the Firepower 2100 mode, Appliance or Platform, use the **show fxos mode** command in privileged EXEC mode.

show fxos mode

Note This command is supported on the Firepower 2100 only.

Syntax Description

This command has no arguments or keywords.

Command Default

The mode is set to Appliance mode by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

The Firepower 2100 runs an underlying operating system called FXOS. You can run the Firepower 2100 in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.
- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Secure Firewall Chassis Manager (formerly Firepower Chassis Manager) web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI.

Use the **show fxos mode** to view the current mode.

Examples

The following is sample output from the **show fxos mode** command:

```
ciscoasa# show fxos mode
Mode is currently set to appliance
```

Related Commands

Command	Description
connect fxos	Connects to the FXOS CLI.
fxos mode appliance	Sets the mode to Appliance mode.

show gc

To display the garbage collection process statistics, use the **show** gc command in privileged EXEC mode.

show gc

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show gc** command:

```
ciscoasa# show gc
Garbage collection process stats:
Total tcp conn delete response            :           0
Total udp conn delete response            :           0
Total number of zombie cleaned            :           0
Total number of embryonic conn cleaned    :           0
Total error response                      :           0
Total queries generated                   :           0
Total queries with conn present response  :           0
Total number of sweeps                    :         946
Total number of invalid vcid              :           0
Total number of zombie vcid               :           0
```

Related Commands

Command	Description
clear gc	Removes the garbage collection process statistics.

show h225

To display information for H.225 sessions established across the ASA, use the show **h225** command in privileged EXEC mode.

show h225

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show h225** command displays information for H.225 sessions established across the ASA.

Before using the **show h225**, **show h245**, or **show h323 ras** commands, we recommend that you configure the **pager** command. If there are a lot of session records and the **pager** command is not configured, it may take a while for the **show** output to reach its end.

If there is an abnormally large number of connections, check that the sessions are timing out based on the default timeout values or the values set by you. If they are not, then there is a problem that needs to be investigated.

Examples

The following is sample output from the **show h225** command:

```
ciscoasa# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
    1. CRV 9861
    Local:   10.130.56.3/1040   Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
    Local:   10.130.56.4/1050   Foreign: 172.30.254.205/1720
```

This output indicates that there is currently 1 active H.323 call going through the ASA between the local endpoint 10.130.56.3 and foreign host 172.30.254.203, and for these particular endpoints, there is 1 concurrent call between them, with a CRV (Call Reference Value) for that call of 9861.

For the local endpoint 10.130.56.4 and foreign host 172.30.254.205, there are 0 concurrent Calls. This means that there is no active call between the endpoints even though the H.225 session still exists. This could happen if, at the time of the **show h225** command, the call has already ended but the H.225 session has not yet been deleted. Alternately, it could mean that the two endpoints still have a TCP connection opened between them because they set "maintainConnection" to TRUE, so the session is kept open until they set it to FALSE again, or until the session times out based on the H.225 timeout value in your configuration.

Related Commands

Commands	Description
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323 ras	Displays information for H.323 RAS sessions established across the ASA.
timeout h225 | h323	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

show h245

To display information for H.245 sessions established across the ASA by endpoints using slow start, use the show **h245** command in privileged EXEC mode.

show h245

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show h245** command displays information for H.245 sessions established across the ASA by endpoints using slow start. (Slow start is when the two endpoints of a call open another TCP control channel for H.245. Fast start is where the H.245 messages are exchanged as part of the H.225 messages on the H.225 control channel.)

Examples

The following is sample output from the **show h245** command:

```
ciscoasa# show h245
Total: 1
        LOCAL           TPKT    FOREIGN         TPKT
1       10.130.56.3/1041        0       172.30.254.203/1245    0
        MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
                      Local   10.130.56.3 RTP 49608 RTCP 49609
        MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
                      Local   10.130.56.3 RTP 49606 RTCP 49607
```

There is currently one H.245 control session active across the ASA. The local endpoint is 10.130.56.3, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0. (The TKTP header is a 4-byte header preceding each H.225/H.245 message. It gives the length of the message, including the 4-byte header.) The foreign host endpoint is 172.30.254.203, and we are expecting the next packet from this endpoint to have a TPKT header because the TPKT value is 0.

The media negotiated between these endpoints have a LCN (logical channel number) of 258 with the foreign RTP IP address/port pair of 172.30.254.203/49608 and a RTCP IP address/port of 172.30.254.203/49609 with a local RTP IP address/port pair of 10.130.56.3/49608 and a RTCP port of 49609.

The second LCN of 259 has a foreign RTP IP address/port pair of 172.30.254.203/49606 and a RTCP IP address/port pair of 172.30.254.203/49607 with a local RTP IP address/port pair of 10.130.56.3/49606 and RTCP port of 49607.

Related Commands

Commands	Description
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.
show h323 ras	Displays information for H.323 RAS sessions established across the ASA.
timeout h225 | h323	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

show h323

To display information for H.323 connections, use the show **h323** command in privileged EXEC mode.

show h323 { **ras | gup** }

Syntax Description

ras	Displays the H323 RAS sessions established across the ASA between a gatekeeper and its H.323 endpoint.
gup	Displays information about the H323 gateway updated protocol connections.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show h323 ras** command displays information for H.323 RAS sessions established across the ASA between a gatekeeper and its H.323 endpoint.

Examples

The following is sample output from the **show h323 ras** command:

```
ciscoasa# show h323 ras
ciscoasa#
Total: 1
        GK                      Caller
        172.30.254.214 10.130.56.14
```

This output shows that there is one active registration between the gatekeeper 172.30.254.214 and its client 10.130.56.14.

Related Commands

Commands	Description
inspect h323	Enables H.323 application inspection.
show h245	Displays information for H.245 sessions established across the ASA by endpoints using slow start.

Commands	Description
timeout h225 | h323	Configures idle time after which an H.225 signaling connection or an H.323 control connection will be closed.

show hardware-bypass

To display the current hardware bypass status on an ISA 3000, use the **show hardware-bypass** command in privileged EXEC mode.

show hardware-bypass

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	—	• Yes	• Yes	—	—

Command History

Release	Modification
9.4(1.225)	This command was added.

Examples

The following is sample output from the **show hardware-bypass** command.

```
ciscoasa# show hardware-bypass

                          Status              Powerdown           Powerup
GigabitEthernet 1/1-1/2   Disable             Disable             Disable
GigabitEthernet 1/3-1/4   Disable             Disable             Disable

Pairing supported on these interfaces: gig1/1 & gig1/2, gig1/3 & gig1/4
```

Related Commands

Commands	Description
hardware-bypass	Configures hardware bypass mode on an ISA 3000 device.

show history

To display the previously entered commands, use the **show history** command in user EXEC mode.

show history

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The show history command lets you display previously entered commands. You can examine commands individually with the up and down arrows, enter ^p to display previously entered lines, or enter ^n to display the next line.

Examples

The following example shows sample output from the **show history** command in user EXEC mode:

```
ciscoasa> show history
show history
help
show history
```

The following example shows sample output from the **show history** command in privileged EXEC mode:

```
ciscoasa
#
 show history
show history
help
show history
enable
show history
```

The following example shows sample output from the **show history** command in global configuration mode:

```
ciscoasa(config)#
show history
show history
help
show history
enable
show history
config t
show history
```

Related Commands

Command	Description
help	Displays help information for the command specified.

show hostname

To show the hostname, use the **show hostname** command in privileged EXEC mode.

show hostname [**fqdn**]

Syntax Description

fqdn	Shows the fully-qualified domain name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	Command added.

Usage Guidelines

Set the hostname using the **hostname** command, and set the domain using the **domain-name** command.

Examples

The following is sample output from the show hostname fqdn command:

```
ciscoasa# show hostname fqdn
asa1.cisco.com
```

Related Commands

Command	Description
hostname	Sets the ASA hostname.
domain-name	Sets the domain name for the ASA.

show icmp

To display the ICMP configuration, use the show icmp command in privileged EXEC mode.

show icmp

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command already existed.

Usage Guidelines

The **show icmp** command displays the ICMP configuration.

Examples

The following example shows the ICMP configuration:

```
ciscoasa# show icmp
```

Related Commands

clear configure icmp	Clears the ICMP configuration.
debug icmp	Enables the display of debugging information for ICMP.
icmp	Configures access rules for ICMP traffic that terminates at an ASA interface.
inspect icmp	Enables or disables the ICMP inspection engine.
timeout icmp	Configures the idle timeout for ICMP.

show idb

To display information about the status of interface descriptor blocks, use the **show idb** command in privileged EXEC mode.

show idb

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

IDBs are the internal data structure representing interface resources. See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show idb** command:

```
ciscoasa# show idb
Maximum number of Software IDBs 280. In use 23.
                   HWIDBs     SWIDBs
            Active 6          21
          Inactive 1          2
        Total IDBs 7          23
 Size each (bytes) 116        212
       Total bytes 812        4876
HWIDB#  1 0xbb68ebc  Control0/0
HWIDB#  2 0xcd47d84  GigabitEthernet0/0
HWIDB#  3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#  4 0xcd5063c  GigabitEthernet0/2
HWIDB#  5 0xcd54a9c  GigabitEthernet0/3
HWIDB#  6 0xcd58f04  Management0/0
SWIDB#  1 0x0bb68f54 0x01010001 Control0/0
SWIDB#  2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#  3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#  1 0x0d44109c 0xffffffff     3  GigabitEthernet0/0.1
  PEER IDB#  2 0x0d2c0674 0x00020002     2  GigabitEthernet0/0.1
  PEER IDB#  3 0x0d05a084 0x00010001     1  GigabitEthernet0/0.1
SWIDB#  4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
```

```
SWIDB#  5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#  6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#  1 0x0cf8686c 0x00020003     2  GigabitEthernet0/1.1
SWIDB#  7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#  1 0x0d2c08ac 0xffffffff     2  GigabitEthernet0/1.2
SWIDB#  8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#  1 0x0d441294 0x00030001     3  GigabitEthernet0/1.3
SWIDB#  9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB# 10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#  1 0x0d3291ec 0x00030002     3  GigabitEthernet0/3
  PEER IDB#  2 0x0d2c0aa4 0x00020001     2  GigabitEthernet0/3
  PEER IDB#  3 0x0d05a474 0x00010002     1  GigabitEthernet0/3
SWIDB# 11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#  1 0x0d05a65c 0x00010003     1  Management0/0
```

Table 7-4 shows each field description.

Table 52: show idb stats Fields

Field	Description
HWIDBs	Shows the statistics for all HWIDBs. HWIDBs are created for each hardware port in the system.
SWIDBs	Shows the statistics for all SWIDBs. SWIDBs are created for each main and subinterface in the system, and for each interface that is allocated to a context. Some other internal software modules also create IDBs.
HWIDB#	Specifies a hardware interface entry. The IDB sequence number, address, and interface name is displayed in each line.
SWIDB#	Specifies a software interface entry. The IDB sequence number, address, corresponding vPif id, and interface name are displayed in each line.
PEER IDB#	Specifies an interface allocated to a context. The IDB sequence number, address, corresponding vPif id, context id and interface name are displayed in each line.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

show igmp groups

To display the multicast groups with receivers that are directly connected to the ASA and that were learned through IGMP, use the **show igmp groups** command in privileged EXEC mode.

show igmp groups [[**reserved** | *group*] [*if_name*] [**detail**]] | **summary**]

Syntax Description

detail	(Optional) Provides a detailed description of the sources.
group	(Optional) The address of an IGMP group. Including this optional argument limits the display to the specified group.
if_name	(Optional) Displays group information for the specified interface.
reserved	(Optional) Displays information about reserved groups.
summary	(Optional) Displays group joins summary information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you omit all optional arguments and keywords, the **show igmp groups** command displays all directly connected multicast groups by group address, interface type, and interface number.

Examples

The following is sample output from the **show igmp groups** command:

```
ciscoasa# show igmp groups
IGMP Connected Group Membership
Group Address    Interface           Uptime    Expires   Last Reporter
224.1.1.1        inside              00:00:53  00:03:26  192.168.1.6
```

Related Commands

Command	Description
show igmp interface	Displays multicast information for an interface.

show igmp interface

To display multicast information for an interface, use the **show igmp interface** command in privileged EXEC mode.

show igmp interface [*if_name*]

Syntax Description

if_name	(Optional) Displays IGMP group information for the selected interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was modified. The **detail** keyword was removed.

Usage Guidelines

If you omit the optional *if_name* argument, the **show igmp interface** command displays information about all interfaces.

Examples

The following is sample output from the **show igmp interface** command:

```
ciscoasa# show igmp interface inside
inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

Related Commands

Command	Description
show igmp groups	Displays the multicast groups with receivers that are directly connected to the ASA and that were learned through IGMP.

show igmp traffic

To display IGMP traffic statistics, use the **show igmp traffic** command in privileged EXEC mode.

show igmp traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show igmp traffic** command:

```
ciscoasa# show igmp traffic
IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                             Received     Sent
Valid IGMP Packets              3          6
Queries                         2          6
Reports                         1          0
Leaves                          0          0
Mtrace packets                  0          0
DVMRP packets                   0          0
PIM packets                     0          0
Errors:
Malformed Packets               0
Martian source                  0
Bad Checksums                   0
```

Related Commands

Command	Description
clear igmp counters	Clears all IGMP statistic counters.
clear igmp traffic	Clears the IGMP traffic counters.

show import webvpn

To list the files, customization objects, translation tables, or plug-ins in flash memory that customize and localize the ASA or the Secure Client, use the **show import webvpn** command in privileged EXEC mode.

show import webvpn { **AnyConnect-customization | customization | mst-translation | plug-in | translation-table | url-list | webcontent** } [**detailed | xml-output**]

Syntax Description

AnyConnect-customization	Displays resource files, executable files, and MS transforms in the ASA flash memory that customize the Secure Client GUI.
customization	Displays XML customization objects in the ASA flash memory that customize the clientless VPN portal (filenames base64 decoded).
mst-translation	Displays MS transforms in the ASA flash memory that translate the Secure Client installer program.
plug-in	Displays plug-in modules in the ASA flash memory (third-party Java-based client applications, including SSH, VNC, and RDP).
translation-table	Displays translation tables in the ASA flash memory that translate the language of user messages displayed by the clientless portal, Secure Desktop, and plug-ins.
url-list	Displays URL lists in the ASA flash memory used by the clientless portal (filenames base64 decoded).
webcontent	Displays content in ASA flash memory used by the clientless portal, clientless applications, and plugins for online help visible to end users.
detailed	Displays the path in flash memory of the file(s) and the hash.
xml-output	Displays the XML of the file(s).

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Release	Modification
8.2(1)	The AnyConnect-customization keyword was added.

Usage Guidelines

Use the **show import webvpn** command to identify the custom data and the Java-based client applications available to clientless SSL VPN users. The displayed list itemizes all of the requested data types that are in flash memory on the ASA.

Examples

The following illustrates the WebVPN data displayed by various **show import webvpn** command:

```
ciscoasa# show import webvpn plug
ssh
rdp
vnc
ciscoasa#
ciscoasa#  show import webvpn plug detail
post GXN2BIGGOAOkBMibDQsMu2GWZ3Q= Tue, 29 Apr 2008 19:57:03 GMT
rdp fHeyReIOUwDCgAL9HdTsPnjdBOo= Tue, 15 Sep 2009 23:23:56 GMT
rdp2 shw8c22T2SsILLk6zyCd6H6VOz8= Wed, 11 Feb 2009 21:17:54 GMT
ciscoasa# show import webvpn customization

Template
DfltCustomization
ciscoasa#
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
  AnyConnect
  PortForwarder
  banners
  csd
  customization
  url-list
  webvpn
Translation Tables:
  ru                                              customization
  ua                                              customization
ciscoasa#
ciscoasa# show import webvpn url-list

Template
No bookmarks are currently defined
ciscoasa#
ciscoasa# show import webvpn webcontent
No custom webcontent is loaded
ciscoasa#
```

Related Commands

Command	Description
revert webvpn all	Removes all WebVPN data and plug-in current on the ASA.

show interface

To view interface statistics, use the **show interface** command in privileged EXEC mode.

show interface [{ *physical_interface* | **redundant** *number* } [*.subinterface*] | *mapped_name* | *interface_name* | **vlan** *number* | **vni** *id* [**summary**]] [**stats** | **detail**]

Syntax Description

detail	(Optional) Shows detailed interface information, including the order in which the interface was added, the configured state, the actual state, and asymmetrical routing statistics, if enabled by the **asr-group** command. If you show all interfaces, then information about the internal interfaces for SSMs displays, if installed on the ASA 5500. The internal interface is not user-configurable, and the information is for debugging purposes only.
interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit ethernet 0/1** . See the **interface** command for accepted values.
redundant *number*	(Optional) Identifies the redundant interface ID, such as **redundant 1** .
stats	(Default) Shows interface information and statistics. This keyword is the default, so this keyword is optional.
summary	(Optional) For a VNI interface, shows only the VNI interface parameters.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For the Firepower 1010, ASA 5505, or ASASM, specifies the VLAN interface.
vni *id*	(Optional) Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.

Command Default

If you do not identify any options, this command shows basic statistics for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was modified to include the new interface numbering scheme, and to add the **stats** keyword for clarity, and the **detail** keyword.
7.0(4)	Support for the 4GE SSM interfaces was added.
7.2(1)	Support for switch interfaces was added.
8.0(2)	Support for redundant interfaces was added. Also, the delay is added for subinterfaces. Two new counters were added: input reset drops and output reset drops.
8.2(1)	The no buffer number was changed to show the number of failures from block allocations.
8.6(1)	Support for the ASA 5512-X through ASA 5555-X shared management interface and the control plane interface for the software module were added. The management interface is displayed using the **show interface detail** command as Internal-Data0/1; the control plane interface is displayed as Internal-Control0/0.
9.4(1)	The **vni** interface type was added.
9.5(1)	Clustering site-specific MAC addresses were added to the output.
9.10(1)	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces.
9.13(1)	We added support for the Firepower 1000 series and Firepower 2100 in Appliance mode.
9.17(1)	For VNI interfaces, shows if single-arm proxy is enabled. For the Secure Firewall 3100, shows the FEC mode and for the **detail** option, the egress interface for a queue.

Usage Guidelines

If an interface is shared among contexts, and you enter this command within a context, the ASA shows only statistics for the current context. When you enter this command in the system execution space for a physical interface, the ASA shows the combined statistics for all contexts.

The number of statistics shown for subinterfaces is a subset of the number of statistics shown for a physical interface.

You cannot use the interface name in the system execution space, because the **nameif** command is only available within a context. Similarly, if you mapped the interface ID to a mapped name using the **allocate-interface** command, you can only use the mapped name in a context. If you set the **visible** keyword in the **allocate-interface** command, the ASA shows the interface ID in the output of the **show interface** command.

Note The number of bytes transmitted or received in the Hardware count and the Traffic Statistics count are different.In the hardware count, the amount is retrieved directly from hardware, and reflects the Layer 2 packet size. While in traffic statistics, it reflects the Layer 3 packet size.The count difference is varied based upon the design of the interface card hardware.For example, for a Fast Ethernet card, the Layer 2 count is 14 bytes greater than the traffic count, because it includes the Ethernet header. On the Gigabit Ethernet card, the Layer 2 count is 18 bytes greater than the traffic count, because it includes both the Ethernet header and the CRC.

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show interface** command:

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Active member of Redundant5
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0)
        output queue (curr/max packets): hardware (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max packets): hardware (128/128) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
Interface Redundant1 "", is down, line protocol is down
  Redundancy Information:
        Members unassigned
Interface Redundant5 "redundant", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c451, MTU 1500
        IP address 10.2.3.5, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (curr/max packets): hardware (0/0) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
  Traffic Statistics for "redundant":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Redundancy Information:
        Member GigabitEthernet0/3(Active), GigabitEthernet0/2
        Last switchover at 15:15:26 UTC Oct 24 2006
Interface Redundant5.1 "", is down, line protocol is down
        VLAN identifier none
        Available but not configured with VLAN or via nameif
```

The following output shows the use of the site MAC address when in use:

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

Table 7-5 shows each field description.

Table 53: show interface Fields

Field	**Description**
Interface *ID*	The interface ID. Within a context, the ASA shows the mapped name (if configured), unless you set the **allocate-interface** command **visible** keyword.
"*interface_name* "	The interface name set with the **nameif** command. In the system execution space, this field is blank because you cannot set the name in the system. If you do not configure a name, the following message appears after the Hardware line: `Available but not configured via nameif`
is *state*	The administrative state, as follows: • up—The interface is not shut down. • administratively down—The interface is shut down with the **shutdown** command.

Field	Description
Line protocol is *state*	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.
VLAN identifier	For subinterfaces, the VLAN ID.
Hardware	The interface type, maximum bandwidth, delay, duplex, and speed. When the link is down, the duplex and speed show the configured values. When the link is up, these fields show the configured values with the actual settings in parentheses. The following list describes the common hardware types: • i82542 - Intel PCI Fiber Gigabit card used on PIX platforms • i82543 - Intel PCI-X Fiber Gigabit card used on PIX platforms • i82546GB - Intel PCI-X Copper Gigabit used on ASA platforms • i82547GI - Intel CSA Copper Gigabit used as backplane on ASA platforms • i82557 - Intel PCI Copper Fast Ethernet used on ASA platforms • i82559 - Intel PCI Copper Fast Ethernet used on PIX platforms • VCS7380 - Vitesse Four Port Gigabit Switch used in SSM-4GE
Media-type	(For 4GE SSM interfaces only) Shows if the interface is set as RJ-45 or SFP.

message area	A message might be displayed in some circumstances. See the following examples:
	• In the system execution space, you might see the following message:
	`Available for allocation to a context`
	• If you do not configure a name, you see the following message:
	`Available but not configured via nameif`
	• If an interface is a member of a redundant interface, you see the following message:
	`Active member of Redundant5`

MAC address	The interface MAC address.
Site Specific MAC address	For clustering, shows an in-use site-specific MAC address.
MTU	The maximum size, in bytes, of packets allowed on this interface. If you do not set the interface name, this field shows “MTU not set.”

Field	Description
IP address	The interface IP address set using the **ip address** command or received from a DHCP server. In the system execution space, this field shows “IP address unassigned” because you cannot set the IP address in the system.
Subnet mask	The subnet mask for the IP address.
Packets input	The number of packets received on this interface.
Bytes	The number of bytes received on this interface.
No buffer	The number of failures from block allocations.
Received:	
Broadcasts	The number of broadcasts received.
Input errors	The number of total input errors, including the types listed below. Other input-related errors can also cause the input error count to increase, and some datagrams might have more than one error; therefore, this sum might exceed the number of errors listed for the types below.
Runts	The number of packets that are discarded because they are smaller than the minimum packet size, which is 64 bytes. Runts are usually caused by collisions. They might also be caused by poor wiring and electrical interference.
Giants	The number of packets that are discarded because they exceed the maximum packet size. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
CRC	The number of Cyclical Redundancy Check errors. When a station sends a frame, it appends a CRC to the end of the frame. This CRC is generated from an algorithm based on the data in the frame. If the frame is altered between the source and destination, the ASA notes that the CRC does not match. A high number of CRCs is usually the result of collisions or a station transmitting bad data.
Frame	The number of frame errors. Bad frames include packets with an incorrect length or bad frame checksums. This error is usually the result of collisions or a malfunctioning Ethernet device.
Overrun	The number of times that the ASA was incapable of handing received data to a hardware buffer because the input rate exceeded the ASA capability to handle the data.
Ignored	This field is not used. The value is always 0.
Abort	This field is not used. The value is always 0.
L2 decode drops	The number of packets dropped because the name is not configured (**nameif** command) or a frame with an invalid VLAN id is received. On a standby interface in a redundant interface configuration, this counter may increase because this interface has no name (**nameif** command) configured.
Packets output	The number of packets sent on this interface.

Field	Description
Bytes	The number of bytes sent on this interface.
Underruns	The number of times that the transmitter ran faster than the ASA could handle.
Output Errors	The number of frames not transmitted because the configured maximum number of collisions was exceeded. This counter should only increment during heavy network traffic.
Collisions	The number of messages retransmitted due to an Ethernet collision (single and multiple collisions). This usually occurs on an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once by the output packets.
Interface resets	The number of times an interface has been reset. If an interface is unable to transmit for three seconds, the ASA resets the interface to restart transmission. During this interval, connection state is maintained. An interface reset can also happen when an interface is looped back or shut down.
Babbles	Unused. ("babble" means that the transmitter has been on the interface longer than the time taken to transmit the largest frame.)
Late collisions	The number of frames that were not transmitted because a collision occurred outside the normal collision window. A late collision is a collision that is detected late in the transmission of the packet. Normally, these should never happen. When two Ethernet hosts try to talk at once, they should collide early in the packet and both back off, or the second host should see that the first one is talking and wait. If you get a late collision, a device is jumping in and trying to send the packet on the Ethernet while the ASA is partly finished sending the packet. The ASA does not resend the packet, because it may have freed the buffers that held the first part of the packet. This is not a real problem because networking protocols are designed to cope with collisions by resending packets. However, late collisions indicate a problem exists in your network. Common problems are large repeated networks and Ethernet networks running beyond the specification.
Deferred	The number of frames that were deferred before transmission due to activity on the link.
input reset drops	Counts the number of packets dropped in the RX ring when a reset occurs.
output reset drops	Counts the number of packets dropped in the TX ring when a reset occurs.
Rate limit drops	(For 4GE SSM interfaces only) The number of packets dropped if you configured the interface at non-Gigabit speeds and attempted to transmit more than 10 Mbps or 100 Mbps, depending on configuration..
Lost carrier	The number of times the carrier signal was lost during transmission.
No carrier	Unused.

Field	Description
Input queue (curr/max packets):	The number of packets in the input queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue. Not available for Gigabit Ethernet interfaces.
Output queue (curr/max packets):	The number of packets in the output queue, the current and the maximum.
Hardware	The number of packets in the hardware queue.
Software	The number of packets in the software queue.
input queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Receive (input) descriptor ring. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.
output queue (blocks free curr/low)	The curr/low entry indicates the number of current and all-time-lowest available slots on the interface's Transmit (output) descriptor rings. These are updated by the main CPU, so the all-time-lowest (until the interface statistics are cleared or the device is reloaded) watermarks are not highly accurate.
Traffic Statistics:	The number of packets received, transmitted, or dropped.
Packets input	The number of packets received and the number of bytes.
Packets output	The number of packets transmitted and the number of bytes.
Packets dropped	The number of packets dropped. Typically this counter increments for packets dropped on the accelerated security path (ASP), for example, if a packet is dropped due to an access list deny. See the **show asp drop** command for reasons for potential drops on an interface.
1 minute input rate	The number of packets received in packets/sec and bytes/sec over the last minute.
1 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last minute.
1 minute drop rate	The number of packets dropped in packets/sec over the last minute.
5 minute input rate	The number of packets received in packets/sec and bytes/sec over the last 5 minutes.
5 minute output rate	The number of packets transmitted in packets/sec and bytes/sec over the last 5 minutes.
5 minute drop rate	The number of packets dropped in packets/sec over the last 5 minutes.

Field	Description
Redundancy Information:	For redundant interfaces, shows the member physical interfaces. The active interface has "(Active)" after the interface ID. If you have not yet assigned members, you see the following output: `Members unassigned`
Last switchover	For redundant interfaces, shows the last time the active interface failed over to the standby interface.

Examples

The following is sample output from the **show interface** command on the ASA 5505, which includes switch ports:

```
ciscoasa# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI, BW 100 Mbps, DLY 100 usec
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps, DLY 1000 usec
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

Table 55: show interface detail Fields shows each field description for the **show interface** command for switch interfaces, such as those for the Firepower 1010 or ASA 5505. See Table 7-6 for fields that are also shown for the **show interface** command.

Table 54: show interface for Switch Interfaces Fields

Field	Description
switch ingress policy drops	This drop is usually seen when a port is not configured correctly. This drop is incremented when a packet cannot be successfully forwarded within switch ports as a result of the default or user configured switch port settings. The following configurations are the likely reasons for this drop: • The **nameif** command was not configured on the VLAN interface. **Note** For interfaces in the same VLAN, even if the **nameif** command was not configured, switching within the VLAN is successful, and this counter does not increment. • The VLAN is shut down. • An access port received an 802.1Q-tagged packet. • A trunk port received a tag that is not allowed or an untagged packet. • The ASA is connected to another Cisco device that has Ethernet keepalives. For example, Cisco IOS software uses Ethernet loopback packets to ensure interface health. This packet is not intended to be received by any other device; the health is ensured just by being able to send the packet. These types of packets are dropped at the switch port, and the counter increments.
switch egress policy drops	Not currently in use.

The following sample output from the **show interface** command for the Secure Firewall 3100 shows the FEC mode as auto using cl74-fc.

```
ciscoasa(config-if)# sh int eth1/5
Interface Ethernet1/5 "", is up, line protocol is up
 Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
   Full-Duplex(fullDuplex), 25000 Mbps(25gbps)
   Available but not configured via nameif
   MAC address fc58.9a06.9112, MTU not set
   IP address unassigned
   FEC mode is auto(cl74-fc)
   13 packets input, 2165 bytes, 0 no buffer
   Received 0 broadcasts, 0 runts, 0 giants
   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
   0 pause input, 0 resume input
   0 packets output, 0 bytes, 0 underruns
   0 pause output, 0 resume output
   0 output errors, 0 collisions, 0 interface resets
   0 late collisions, 0 deferred
   0 input reset drops, 0 output reset drops
```

Examples

The following is sample output from the **show interface detail** command. The following example shows detailed interface statistics for all interfaces, including the internal interfaces (if present for your platform) and asymmetrical routing statistics, if enabled by the **asr-group** command:

```
ciscoasa# show interface detail
```

```
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 1000 usec
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/7)
        output queue (curr/max packets): hardware (0/13)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max packets): hardware (0/2) software (0/0)
        output queue (curr/max packets): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

Table 55: show interface detail Fields shows each field description for the **show interface detail** command. See Table 55: show interface detail Fields for fields that are also shown for the **show interface** command.

Table 55: show interface detail Fields

Field	Description
Demux drops	(On Internal-Data interface only) The number of packets dropped because the ASA was unable to demultiplex packets from SSM interfaces. SSM interfaces communicate with the native interfaces across the backplane, and packets from all SSM interfaces are multiplexed on the backplane.
Control Point Interface States:	
Interface number	A number used for debugging that indicates in what order this interface was created, starting with 0.

Field	Description
Interface config status	The administrative state, as follows: • active—The interface is not shut down. • not active—The interface is shut down with the **shutdown** command.
Interface state	The actual state of the interface. In most cases, this state matches the config status above. If you configure high availability, it is possible there can be a mismatch because the ASA brings the interfaces up or down as needed.
Asymmetrical Routing Statistics:	
Received X1 packets	Number of ASR packets received on this interface.
Transmitted X2 packets	Number of ASR packets sent on this interfaces.
Dropped X3 packets	Number of ASR packets dropped on this interface. The packets might be dropped if the interface is down when trying to forward the packet.

The following is sample output from the **show interface detail** command on the ASA 5512-X through ASA 5555-X, which shows combined statistics for the Management 0/0 interface (shown as “Internal-Data0/1”) for both the ASA and the software module. The output also shows the Internal-Control0/0 interface, which is used for control traffic between the software module and the ASA.

```
Interface Internal-Data0/1 "ipsmgmt", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "ipsmgmt":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
Interface Internal-Control0/0 "cplane", is down, line protocol is up
  Hardware is , BW Unknown Speed-Capability, DLY 1000 usec
        (Full-duplex), (1000 Mbps)
        Input flow control is unsupported, output flow control is unsupported
        MAC address 0100.0100.0000, MTU not set
        IP address 127.0.1.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        182 packets output, 9992 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "cplane":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 11
        Interface config status is active
        Interface state is active
```

See the following output for **show interface detail** for the Secure Firewall 3100 showing the egress interface for a queue:

```
ciscoasa# show interface detail
Interface Internal Data0/1 "", is up, line protocol is up
   Hardware is , BW 500000 Mbps, DLY 1000 usec
      (Full duplex), (50000 Mbps)
      [...]
         TX[64]: 0 packets, 0 bytes, 0 underruns
            Blocks free curr /low: 511/512
            Used by Ethernet1/1
         TX[65]: 0 packets, 0 bytes, 0 underruns
            Blocks free curr /low: 511/512
            Used by Ethernet1/1
```

See the following output for the **show interface vni 1** command:

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
```

```
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

See the following output for the **show interface vni 1 summary** command:

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear interface	Clears counters for the **show interface** command.
delay	Changes the delay metric for an interface.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show interface ip brief

To view interface IP addresses and status, use the **show interface ip brief** command in privileged EXEC mode.

show interface [*physical_interface* [*.subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] **ip brief**

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit ethernet0/1** . See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Command Default

If you do not specify an interface, the ASA shows all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	Support for VLAN interfaces and for the Management 0/0 interface or subinterface in transparent mode was added.
9.10(1)	Support for supervisor association for the Firepower 2100/4100/9300 devices was added.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name or the interface name in a context.

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ip brief** command:

```
ciscoasa# show interface ip brief
    Interface                  IP-Address      OK? Method  Status                Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   admin  down            down
    GigabitEthernet0/2         10.1.1.50       YES manual  admin down            down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    admin down            down
    Management0/0              209.165.201.3   YES CONFIG  up
The following is sample output from the show ip brief
command on ASA with FXOS:
ciscoasa# sh int ip br
Interface                  IP-Address      OK?           Method Status       Protocol
Internal-Data0/0           unassigned      YES           unset  up           up
Vlan10                     172.18.249.190  YES           CONFIG up           up
Vlan80                     80.1.1.1        YES           manual up           up
Vlan300                    14.30.1.1       YES           CONFIG up           up
....
Ethernet1/1                unassigned      YES           unset  up           up
Ethernet1/2                unassigned      YES           unset  down         down
Ethernet1/3                unassigned      unassociated  unset  admin down   down
Ethernet1/4                unassigned      unassociated  unset  admin down   down
Ethernet1/5                unassigned      YES           unset  up           up
Ethernet1/6                unassigned      unassociated  unset  down         down
Ethernet1/7                unassigned      unassociated  unset  down         down
Ethernet1/8                unassigned      unassociated  unset  up           up
Internal-Data1/1           169.254.1.1     YES           unset  up           up
Management1/1              unassigned      YES           unset  up           up
BVI50                      50.1.1.3        YES           CONFIG up           up
Port-channel3              unassigned      YES           unset  down         down
Port-channel8              8.0.0.1         YES           manual up           up
```

Examples

Table 55: show interface detail Fields shows each field description.

Table 56: show interface ip brief Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command. If you show all interfaces, then information about the internal interface for the AIP SSM displays, if installed on the ASA. The internal interface is not user-configurable, and the information is for debugging purposes only.
IP-Address	The interface IP address.
OK?	This column displays "YES" if the interface is associated with supervisor; displays “unassociated” if the interface is not associated with supervisor. This state is applicable only for Firepower 2100/4100/9300 interfaces and devices. For FXOS-based ASA devices, this column displays “unassociated” when interfaces are added to the port channels. For other devices, this column is not currently used, and always shows “YES”.

Field	Description
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.
Status	The administrative state, as follows: • up—The interface is not shut down. • admin down—The interface is shut down with the **shutdown** command.
Protocol	The line status, as follows: • up—A working cable is plugged into the network interface. • down—Either the cable is incorrect or not plugged into the interface connector.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.

show inventory

To display information about all of the Cisco products installed in the networking device that are assigned a product identifier (PID), version identifier (VID), and serial number (SN), use the **show inventory** command in user EXEC mode.

show inventory *mod_id*

Syntax Description

mod_id	(Optional) Specifies the module ID or slot number, 0-3.

Command Default

If you do not specify a slot to show inventory for an item, the inventory information of all modules (including the power supply) is displayed.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was introduced.
8.4(2)	The output for an SSP was added. In addition, support for a dual SSP installation was added.
8.6(1)	The output for the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X (the chassis, redundant power supplies, and I/O expansion card) was added.
9.1(1)	The output for the ASA CX module was added.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI, which is a combination of three separate data elements: the product identifier (PID), the version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that you use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product has a unique serial number assigned at the factory, which cannot be changed in the field. The serial number is the means by which to identify an individual, specific instance of a product. The serial number can be different lengths for the various components of the device.

The UDI refers to each product as an entity. Some entities, such as a chassis, have sub-entities like slots. Each entity appears on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the **show inventory** command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

Note When two SSPs are installed in the same chassis, the number of the module indicates the physical location of the module in the chassis. The chassis master is always the SSP installed in slot 0. Only those sensors with which the SSP is associated are displayed in the output.The term *module* in the output is equivalent to physical slot. In the description of the SSP itself, the output includes module: 0 when it is installed in physical slot 0, and module: 1 otherwise. When the target SSP is the chassis master, the **show inventory** command output includes the power supplies and/or cooling fans. Otherwise, these components are omitted.

The serial number may not display because of hardware limitations on the ASA 5500-X series. For the UDI display of the PCI-E I/O (NIC) option cards in these models, there are six possible outputs according to the chassis type, although there are only two different card types. This is because there are different PCI-E bracket assemblies used according to the specified chassis. The following examples show the expected outputs for each PCI-E I/O card assembly. For example, if a Silicom SFP NIC card is detected, the UDI display is determined by the device on which it is installed. The VID and S/N values are N/A, because there is no electronic storage of these values.

For a 6-port SFP Ethernet NIC card in an ASA 5512-X or 5515-X:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-A    , VID: N/A, SN: N/A
```

For a 6-port SFP Ethernet NIC card in an ASA 5525-X:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-B    , VID: N/A, SN: N/A
```

For a 6-port SFP Ethernet NIC card in an ASA 5545-X or 5555-X:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port GE SFP, SX/LX"
PID: ASA-IC-6GE-SFP-C    , VID: N/A, SN: N/A
```

For a 6-port Copper Ethernet NIC card in an ASA 5512-X or 5515-X:

```
Name: "module1", DESCR: "ASA 5512-X/5515-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-A    , VID: N/A, SN: N/A
```

For a 6-port Copper Ethernet NIC card in an ASA 5525-X:

```
Name: "module1", DESCR: "ASA 5525-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-B    , VID: N/A, SN: N/A
```

For a 6-port Copper Ethernet NIC card in an ASA 5545-X or 5555-X:

```
Name: "module1", DESCR: "ASA 5545-X/5555-X Interface Card 6-port 10/100/1000, RJ-45"
PID: ASA-IC-6GE-CU-C    , VID: N/A, SN: N/A
```

Examples

The following is sample output from the **show inventory** command without any keywords or arguments. This sample output displays a list of Cisco entities installed in an ASA that are each assigned a PID, including a storage device used for an ASA CX module.

```
ciscoasa> show inventory

Name: "Chassis", DESCR: "ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt"
PID: ASA5555           , VID: V01     , SN: FGL170441BU
Name: "power supply 1", DESCR: "ASA 5545-X/5555-X AC Power Supply"
PID: ASA-PWR-AC        , VID: N/A     , SN: 2CS1AX
Name: "Storage Device 1", DESCR: "Micron 128 GB SSD MLC, Model Number: C400-MTFDDAC128MAM"
PID: N/A               , VID: N/A     , SN: MXA174201RR
```

The following example shows the output of the **show inventory** command on a chassis master for a dual SSP installation:

```
ciscoasa> show inventory

Name: "module 0", DESCR: "ASA 5585-X Security Services Processor-40 w 6GE,4 SFP+"
PID: ASA5585-SSP-40    , VID: V01     , SN: JAF1436ACLJ
Name: "Chassis", DESCR: "ASA 5585-X"
PID: ASA5585           , VID: V01     , SN: 123456789AB
Name: "fan", DESCR: "ASA 5585-X Fan Module"
PID: ASA5585-FAN       , VID: V01     , SN: POG1434000G
Name: "power supply 0", DESCR: "ASA 5585-X AC Power Supply"
PID: ASA5585-PWR-AC    , VID: V01     , SN: POG1434002K
```

This command only shows removable modules. Thus, though **show interface brief** in ASA shows all the SFP interfaces in EPM, the **show inventory** command in ASA would only show data for interfaces that have an SFP plugged in. The following example shows the output of the **show inventory** command on SFP interface that is plugged in:

```
ciscoasa> show inventory

Name: "Ethernet 1/13", DESCR: "h10g-acu1m"
PID: SFP-10G-AOC1M, VID: , SN: A4Z1942K0UC-B
```

Table 7-9 describes the fields shown in the display.

Table 57: Field Descriptions for show inventory

Field	Description
Name	Physical name (text string) assigned to the Cisco entity. For example, console, SSP, or a simple component number (port or module number), such as "1," depending on the physical component naming syntax of the device. Equivalent to the entPhysicalName MIB variable in RFC 2737.
DESCR	Physical description of the Cisco entity that characterizes the object. Equivalent to the entPhysicalDesc MIB variable in RFC 2737.
PID	Entity product identifier. Equivalent to the entPhysicalModelName MIB variable in RFC 2737.
VID	Entity version identifier. Equivalent to the entPhysicalHardwareRev MIB variable in RFC 2737.
SN	Entity serial number. Equivalent to the entPhysicalSerialNum MIB variable in RFC 2737.

Related Commands

Command	Description
show diag	Displays diagnostic information about the controller, interface processor, and port adapters for a networking device.
show tech-support	Displays general information about the router when it reports a problem.

show ip address

To view interface IP addresses or, for transparent mode, the management IP address, use the **show ip address** command in privileged EXEC mode.

show ip address [*physical_interface* [*.subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

Syntax Description

interface_name	(Optional) Identifies the interface name set with the **nameif** command.
mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Command Default

If you do not specify an interface, the ASA shows all interface IP addresses.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	Support for VLAN interfaces was added.

Usage Guidelines

This command shows the primary IP addresses (called “System” in the display) for when you configure high availability as well as the current IP addresses. If the unit is active, then the system and current IP addresses match. If the unit is standby, then the current IP addresses show the standby addresses.

Examples

The following is sample output from the **show ip address** command:

```
ciscoasa# show ip address
System IP Addresses:
Interface                 Name         IP address      Subnet mask      Method
```

```
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
```

Table 55: show interface detail Fields shows each field description.

Table 58: show ip address Fields

Field	Description
Interface	The interface ID or, in multiple context mode, the mapped name if you configured it using the **allocate-interface** command.
Name	The interface name set with the **nameif** command.
IP address	The interface IP address.
Subnet mask	The IP address subnet mask.
Method	The method by which the interface received the IP address. Values include the following: • unset—No IP address configured. • manual—Configured the running configuration. • CONFIG—Loaded from the startup configuration. • DHCP—Received from a DHCP server.

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface	Displays the runtime status and statistics of interfaces.
show interface ip brief	Shows the interface IP address and status.

show ip address dhcp

To view detailed information about the DHCP lease or server for an interface, use the **show ip address dhcp** command in privileged EXEC mode.

show ip address { *physical_interface* [*.subinterface*] | *mapped_name* | *interface_name* } **dhcp** { **lease** | **server** }
show ip address { *physical_interface* [*.subinterface*] | *mapped_name* | *interface_name* } **dhcp lease** { **proxy** | **server** } { **summary** }

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
lease	Shows information about the DHCP lease.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabit ethernet0/1** . See the **interface** command for accepted values.
proxy	Shows proxy entries in the IPL table.
server	Shows server entries in the IPL table.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.
summary	Shows summary for the entry.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **lease** and **server** keywords to accommodate the new server functionality were added.
7.2(1)	Support for VLAN interfaces and for the Management 0/0 interface or subinterface in transparent mode was added.
9.1(4)	The proxy and summary keywords to accommodate the new server functionality were added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ip address dhcp lease** command:

```
ciscoasa# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

Table 55: show interface detail Fields shows each field description.

Table 59: show ip address dhcp lease Fields

Field	Description
Temp IP Addr	The IP address assigned to the interface.
Temp sub net mask	The subnet mask assigned to the interface.
DHCP Lease server	The DHCP server address.
state	The state of the DHCP lease, as follows: • Initial—The initialization state, where the ASA begins the process of acquiring a lease. This state is also shown when a lease ends or when a lease negotiation fails. • Selecting—The ASA is waiting to receive DHCPOFFER messages from one or more DHCP servers, so it can choose one. • Requesting—The ASA is waiting to hear back from the server to which it sent its request. • Purging—The ASA is removing the lease because the client has released the IP address or there was some other error. • Bound—The ASA has a valid lease and is operating normally. • Renewing—The ASA is trying to renew the lease. It regularly sends DHCPREQUEST messages to the current DHCP server, and waits for a reply. • Rebinding—The ASA failed to renew the lease with the original server, and now sends DHCPREQUEST messages until it gets a reply from any server or the lease ends. • Holddown—The ASA started the process to remove the lease. • Releasing—The ASA sends release messages to the server indicating that the IP address is no longer needed.

Field	Description
DHCP transaction id	A random number chosen by the client, used by the client and server to associate the request messages.
Lease	The length of time, specified by the DHCP server, that the interface can use this IP address.
Renewal	The length of time until the interface automatically attempts to renew this lease.
Rebind	The length of time until the ASA attempts to rebind to a DHCP server. Rebinding occurs if the ASA cannot communicate with the original DHCP server, and 87.5 percent of the lease time has expired. The ASA then attempts to contact any available DHCP server by broadcasting DHCP requests.
Temp default-gateway addr	The default gateway address supplied by the DHCP server.
Temp ip static route0	The default static route.
Next timer fires after	The number of seconds until the internal timer triggers.
Retry count	If the ASA is attempting to establish a lease, this field shows the number of times the ASA tried sending a DHCP message. For example, if the ASA is in the Selecting state, this value shows the number of times the ASA sent discover messages. If the ASA is in the Requesting state, this value shows the number of times the ASA sent request messages.
Client-ID	The client ID used in all communication with the server.
Proxy	Specifies if this interface is a proxy DHCP client for VPN clients, True or False.
Proxy Network	The requested network.
Hostname	The client hostname.

The following is sample output from the **show ip address dhcp server** command:

```
ciscoasa# show ip address outside dhcp server
   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

Table 7-12 shows each field description.

Table 60: show ip address dhcp server Fields

Field	Description
DHCP server	The DHCP server address from which this interface obtained a lease. The top entry ("ANY") is the default server and is always present.
Leases	The number of leases obtained from the server. For an interface, the number of leases is typically 1. If the server is providing address for an interface that is running proxy for VPN, there will be several leases.
Offers	The number of offers from the server.
Requests	The number of requests sent to the server.
Acks	The number of acknowledgments received from the server.
Naks	The number of negative acknowledgments received from the server.
Declines	The number of declines received from the server.
Releases	The number of releases sent to the server.
Bad	The number of bad packets received from the server.
DNS0	The primary DNS server address obtained from the DHCP server.
DNS1	The secondary DNS server address obtained from the DHCP server.
WINS0	The primary WINS server address obtained from the DHCP server.
WINS1	The secondary WINS server address obtained from the DHCP server.
Subnet	The subnet address obtained from the DHCP server.
DNS Domain	The domain obtained from the DHCP server.

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip address pppoe

To view detailed information about the PPPoE connection, use the **show ip address pppoe** command in privileged EXEC mode.

show ip address { *physical_interface* [*.subinterface*] | *mapped_name* | *interface_name* | **vlan** *number* } **pppoe**

Syntax Description

interface_name	Identifies the interface name set with the **nameif** command.
mapped_name	In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	Identifies the interface ID, such as **gigabitethernet0/1**. See the **interface** command for accepted values.
subinterface	Identifies an integer between 1 and 4294967293 designating a logical subinterface.
vlan *number*	(Optional) For models with a built-in switch, such as the ASA 5505 adaptive security appliance, specifies the VLAN interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ip address pppoe** command:

```
ciscoasa# show ip address outside pppoe
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.

Command	Description
ip address ppoe	Sets the interface to obtain an IP address from a PPPoE server.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.
show ip address	Displays the IP addresses of interfaces.

show ip audit count

To show the number of signature matches when you apply an audit policy to an interface, use the **show ip audit count** command in privileged EXEC mode.

show ip audit count [**global** | **interface** *interface_name*]

Syntax Description

global	(Default) Shows the number of matches for all interfaces.
interface *interface_name*	(Optional) Shows the number of matches for the specified interface.

Command Default

If you do not specify a keyword, this command shows the matches for all interfaces (**global**).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

To create an audit policy, use the **ip audit name** command, and to apply the policy, use the **ip audit interface** command.

Examples

The following is sample output from the **show ip audit count** command:

```
ciscoasa# show ip audit count
IP AUDIT GLOBAL COUNTERS
1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
```

```
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 I DNS Host Info              0
6051 I DNS Zone Xfer              0
6052 I DNS Zone Xfer High Port    0
6053 I DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0
IP AUDIT INTERFACE COUNTERS: inside
...
```

Related Commands

Command	Description
clear ip audit count	Clears the count of signature matches for an audit policy.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

show ip local pool

To display IPv4 address pool information, use the **show ip local pool** command in privileged EXEC mode.

show ip local pool interface *pool_name*

Syntax Description

pool_name	The name of the address pool. Enter ? to see a list of pools.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use this command to view the contents of IPv4 address pools created using the **ip local pool** command. These pools are used with remote access VPN and clustering. Use the **ipv6 local pool** command to view IPv6 address pools.

Examples

The following is sample output from the **show ipv6 local pool** command:

```
ciscoasa# show ip local pool test-ipv4-pool

Begin           End             Mask            Free     Held     In use
10.100.10.10    10.100.10.254   255.255.255.0     245        0        0
Available Addresses:
10.100.10.10
10.100.10.11
10.100.10.12
10.100.10.13
10.100.10.14
10.100.10.15
10.100.10.16
... (remaining output redacted)...
```

Related Commands

Command	Description
ip local pool	Configures an IPv4 address pool.

show ip verify statistics

To show the number of packets dropped because of the Unicast RPF feature, use the **show ip verify statistics** command in privileged EXEC mode. Use the **ip verify reverse-path** command to enable Unicast RPF.

show ip verify statistics [**interface** *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Shows statistics for the specified interface.

Command Default

This command shows statistics for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show ip verify statistics** command:

```
ciscoasa# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
ip verify reverse-path	Enables the Unicast Reverse Path Forwarding feature to prevent IP spoofing.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

show ips

To show all available IPS virtual sensors that are configured on the AIP SSM, use the **show ips** command in privileged EXEC mode.

show ips [**detail**]

Syntax Description

detail	(Optional) Shows the sensor ID number as well as the name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

In multiple context mode, this command shows all virtual sensors when entered in the system execution space, but only shows the virtual sensors assigned to the context in the context execution space. See the **allocate-ips** command to assign virtual sensors to contexts.

Virtual sensors are available in IPS Version 6.0 and above.

Examples

The following is sample output from the **show ips** command:

```
ciscoasa# show ips
Sensor name
------------
ips1
ips2
```

The following is sample output from the **show ips detail** command:

```
ciscoasa# show ips detail
Sensor name            Sensor ID
------------           ---------
ips1                   1
ips2                   2
```

Related Commands

Command	Description
allocate-ips	Assigns a virtual sensor to a security context.
ips	Diverts traffic to the AIP SSM.

show ipsec df-bit

To display the IPsec do-not-fragment (DF-bit) policy for IPsec packets for a specified interface, use the **show ipsec df-bit** command in global configuration mode and privileged EXEC mode. You can also use the command synonym **show crypto ipsec df-bit**.

show ipsec df-bit *interface*

Syntax Description

interface	Specifies an interface name.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The df-bit setting determines how the system handles the do-not-fragment (DF) bit in the encapsulated header. The DF bit within the IP header determines whether or not a device is allowed to fragment a packet. Based on this setting, the system either clears, sets, or copies the DF-bit setting of the clear-text packet to the outer IPsec header when applying encryption.

Examples

The following example displays the IPsec DF-bit policy for interface named inside:

```
ciscoasa(config)# show
 ipsec df-bit inside
df-bit inside copy
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec df-bit	Configures the IPsec DF-bit policy for IPsec packets.
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.

Command	Description
show crypto ipsec fragmentation	Displays the fragmentation policy for IPsec packets.

show crypto ipsec fragmentation

To display the fragmentation policy for IPsec packets, use the **show ipsec fragmentation** command in global configuration or privileged EXEC mode. You can also use the command synonym **show crypto ipsec fragmentation**.

show ipsec fragmentation *interface*

Syntax Description

interface	Specifies an interface name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When encrypting packets for a VPN, the system compares the packet length with the MTU of the outbound interface. If encrypting the packet will exceed the MTU, the packet must be fragmented. This command shows whether the system will fragment the packet after encrypting it (after-encryption), or before encrypting it (before-encryption). Fragmenting the packet before encryption is also called prefragmentation, and is the default system behavior because it improves overall encryption performance.

Examples

The following example, entered in global configuration mode, displays the IPsec fragmentation policy for an interface named inside:

```
ciscoasa(config)# show ipsec fragmentation inside
fragmentation inside before-encryption
ciscoasa(config)#
```

Related Commands

Command	Description
crypto ipsec fragmentation	Configures the fragmentation policy for IPsec packets.
crypto ipsec df-bit	Configures the DF-bit policy for IPsec packets.

Command	Description
show ipsec df-bit	Displays the DF-bit policy for a specified interface.

show ipsec policy

To display IPsec secure socket API (SS API) security policy configured for OSPFv3, use the **show ipsec policy** command in global configuration or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec policy**.

show ipsec policy

Syntax Description

This command has no keywords or variables.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	—
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following example shows the OSPFv3 authentication and encryption policy.

```
ciscoasa# show ipsec policy

Crypto IPsec client security policy data
Policy name:      OSPFv3-1-256
Policy refcount:  1
Policy flags:     0x00000000
SA handles:       sess 268382208 (0xfff3000) / in 55017 (0xd6e9) / out 90369 (0x16101)
Inbound  ESP SPI:        256 (0x100)
Outbound ESP SPI:        256 (0x100)
Inbound  ESP Auth Key:   1234567890123456789012345678901234567890
Outbound ESP Auth Key:   1234567890123456789012345678901234567890
Inbound  ESP Cipher Key: 12345678901234567890123456789012
Outbound ESP Cipher Key: 12345678901234567890123456789012
Transform set:    esp-aes esp-sha-hmac
```

Related Commands

Command	Description
ipv6 ospf encryption	Configures the authentication and encryption policy for OSPFv3.
show crypto sockets	Displays secure socket information.

Command	Description
show ipv6 ospf interface	Displays information about OSPFv3 interfaces.

show ipsec sa

To display a list of IPsec SAs, use the **show ipsec sa** command in global configuration mode or privileged EXEC mode. You can also use the alternate form of this command: **show crypto ipsec sa** .

show ipsec sa [**assigned-address** *hostname or IP address* | **entry** | **identity** | **inactive** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

Syntax Description

assigned-address	(Optional) Displays IPsec SAs for the specified hostname or IP address.
detail	(Optional) Displays detailed error information on what is displayed.
entry	(Optional) Displays IPsec SAs sorted by peer address
identity	(Optional) Displays IPsec SAs for sorted by identity, not including ESPs. This is a condensed form.
inactive	(Optional) Displays IPsec SAs that are unable to pass traffic.
map *map-name*	(Optional) Displays IPsec SAs for the specified crypto map.
peer *peer-addr*	(Optional) Displays IPsec SAs for specified peer IP addresses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for OSPFv3 and multiple context mode was added.
9.1(4)	Output has been updated to reflect the assigned IPv6 address and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic.

Examples

The following example, entered in global configuration mode, displays IPsec SAs, including the assigned IPv6 address and the Tansport Mode and GRE encapsulation indication.

```
ciscoasa(config)# sho ipsec sa
interface: outside
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 18, #pkts decrypt: 18, #pkts verify: 18
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 4
     local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624
    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x0003FFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28387
         IV size: 8 bytes
        replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

The following example, entered in global configuration mode, displays IPsec SAs, including an in-use setting to identify a tunnel as OSPFv3.

```
ciscoasa(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3),}
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={L2L, Transport, Manual key (OSPFv3), }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    Crypto map tag: def, local addr: 10.132.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
ciscoasa(config)#
```

Note Fragmentation statistics are pre-fragmentation statistics if the IPsec SA policy states that fragmentation occurs before IPsec processing. Post-fragmentation statistics appear if the SA policy states that fragmentation occurs after IPsec processing.

The following example, entered in global configuration mode, displays IPsec SAs for a crypto map named def.

```
ciscoasa(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
```

```
          slot: 0, conn_id: 3, crypto-map: def
          sa timing: remaining key lifetime (sec): 480
          IV size: 8 bytes
          replay detection support: Y
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

The following example, entered in global configuration mode, shows IPsec SAs for the keyword **entry** .

```
ciscoasa(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
```

```
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

The following example, entered in global configuration mode, shows IPsec SAs with the keywords **entry detail** .

```
ciscoasa(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
ciscoasa(config)#
```

The following example shows IPsec SAs with the keyword **identity** .

```
ciscoasa(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example shows IPsec SAs with the keywords **identity** and **detail** .

```
ciscoasa(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68
    Crypto map tag: def, local addr: 172.20.0.17
      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0
      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0
      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8
      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

The following example displays IPSec SAs based on IPv6 assigned address:

```
ciscoasa(config)# sho ipsec sa assigned-address 2001:1000::10
assigned address: 2001:1000::10
    Crypto map tag: def, seq num: 1, local addr: 75.2.1.23
      local ident (addr/mask/prot/port): (75.2.1.23/255.255.255.255/47/0)
      remote ident (addr/mask/prot/port): (75.2.1.60/255.255.255.255/47/0)
      current_peer: 75.2.1.60, username: rashmi
      dynamic allocated peer ip: 65.2.1.100
      dynamic allocated peer ip(ipv6): 2001:1000::10
      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 326, #pkts decrypt: 326, #pkts verify: 326
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #post-frag successes: 0, #post-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0      #TFC
rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 35
      local crypto endpt.: 75.2.1.23/4500, remote crypto endpt.: 75.2.1.60/64251
      path mtu 1342, ipsec overhead 62(44), override mtu 1280, media mtu 1500
      PMTU time remaining (sec): 0, DF policy: copy-df
      ICMP error validation: disabled, TFC packets: disabled
      current outbound spi: D9C00FC2
      current inbound spi : 4FCB6624
    inbound esp sas:
      spi: 0x4FCB6624 (1338730020)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0xFFFFFFFF 0xFFFFFFFF
    outbound esp sas:
      spi: 0xD9C00FC2 (3653242818)
         transform: esp-3des esp-sha-hmac no compression
         in use settings ={RA, Transport,  NAT-T-Encaps, GRE, IKEv2, }
         slot: 0, conn_id: 8192, crypto-map: def
         sa timing: remaining key lifetime (sec): 28108
         IV size: 8 bytes
         replay detection support: Y
         Anti replay bitmap:
          0x00000000 0x00000001
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config isakmp	Displays all the active ISAKMP configuration.

show ipsec sa summary

To display a summary of IPsec SAs, use the **show ipsec sa summary** command in global configuration mode or privileged EXEC mode.

show ipsec sa summary

Syntax Description

This command has no arguments or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following example, entered in global configuration mode, displays a summary of IPsec SAs by the following connection types:

- IPsec
- IPsec over UDP
- IPsec over NAT-T
- IPsec over TCP
- IPsec VPN load balancing

```
ciscoasa(config)# show ipsec sa summary
Current IPsec SA's:            Peak IPsec SA's:
IPsec            :     2         Peak Concurrent SA  :    14
IPsec over UDP   :     2         Peak Concurrent L2L :     0
IPsec over NAT-T :     4         Peak Concurrent RA  :    14
IPsec over TCP   :     6
IPsec VPN LB     :     0
```

```
Total            :    14
ciscoasa(config)#
```

Related Commands

Command	Description
clear ipsec sa	Removes IPsec SAs entirely or based on specific parameters.
show ipsec sa	Displays a list of IPsec SAs.
show ipsec stats	Displays a list of IPsec statistics.

show ipsec stats

To display a list of IPsec statistics, use the **show ipsec stats** command in global configuration mode or privileged EXEC mode.

show ipsec stats

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	ESPv3 statistics are shown with IPsec subsystems, and support for multiple context mode was added.

Usage Guidelines

The following table describes what the output entries indicate.

Output	Description
IPsec Global Statistics	This section pertains to the total number of IPsec tunnels that the ASA supports.
Active tunnels	The number of IPsec tunnels that are currently connected.
Previous tunnels	The number of IPsec tunnels that have been connected, including the active ones.
Inbound	This section pertains to inbound encrypted traffic that is received through IPsec tunnels.
Bytes	The number of bytes of encrypted traffic that has been received.

Output	Description
Decompressed bytes	The number of bytes of encrypted traffic that were received after decompression was performed, if applicable. This counter should always be equal to the previous one if compression is not enabled.
Packets	The number of encrypted IPsec packets that were received.
Dropped packets	The number of encrypted IPsec packets that were received and dropped because of errors.
Replay failures	The number of anti-replay failure that were detected on received, encrypted IPsec packets.
Authentications	The number of successful authentications performed on received, encrypted IPsec packets.
Authentication failures	The number of authentications failure detected on received, encrypted IPsec packets.
Decryptions	The number of successful decryptions performed on received, encrypted IPsec packets.
Decryption failures	The number of decryptions failures detected on received, encrypted IPsec packets.
Decapsulated fragments needing reassembly	The number of decryption IPsec packets that include IP fragments to be reassembled.
Outbound	This section pertains to outbound cleartext traffic to be transmitted through IPsec traffic.
Bytes	The number of bytes of cleartext traffic to be encrypted and transmitted through IPsec tunnels.
Uncompressed bytes	The number of bytes of uncompressed cleartext traffic to be encrypted and transmitted through IPsec tunnels. The counter should always be equal to the previous one if compression is not enabled
Packets	The number of cleartext packets to be encrypted and transmitted through IPsec tunnels.
Dropped packets	The number of cleartext packets to be encrypted and transmitted through IPsec tunnels that have been dropped because of errors.
Authentications	The number of successful authentications performed on packets to be transmitted through IPsec tunnels.
Authentication failures	The number of authentication failures that were detected on packets to be transmitted through IPsec tunnels.
Encryptions	The number of successful encryptions that were performed on packets to be transmitted through IPsec tunnels.

Output	Description
Encryption failures	The number of encryption failures that were detected on packets to be transmitted through IPsec tunnels.
Fragmentation successes	The number of successful fragmentation operations that were performed as part of outbound IPsec packet transformation.
Pre-fragmentation successes	The number of successful prefragmentation operations that were performed as part of outbound IPsec packet transformation. Prefragmentation occurs before the cleartext packet is encrypted and encapsulated as one or more IPsec packets.
Post-fragmentation successes	The number of successful prefragmentation operations that were performed as part of outbound IPsec packet transformation. Post-fragmentation occurs after the cleartext packet is encrypted and encapsulated as an IPsec packet, which results in multiple IP fragments. These fragments must be reassembled before decryption.
Fragmentation failures	The number of fragmentation failures that have occurred during outbound IPsec packet transformation.
Pre-fragmentation failures	The number of prefragmentation failures that have occurred during outbound IPsec packet transformation. Prefragmentation occurs before the cleartext packet is encrypted and encapsulated as one or more IPsec packets.
Post-fragmentation failure	The number of post-fragmentation failure that have occurred during outbound IPsec packet transformation. Post-fragmentation occurs after the cleartext packet is encrypted and encapsulated as an IPsec packet, which results in multiple IP fragments. These fragments must be reassembled before decryption.
Fragments created	The number of fragments that were created as part of IPsec transformation.
PMTUs sent	The number of path MTU messages that were sent by the IPsec system. IPsec will send a PMTU message to an inside host that is sending packets that are too large to be transmitted through an IPsec tunnel after encapsulation. The PMTU message is a request for the host to lower its MTU and send smaller packets for transmission through the IPsec tunnel.
PMTUs recvd	The number of path MTU messages that were received by the IPsec system. IPsec will receive a path MTU message from a downstream network element if the packets it is sending through the tunnel are too large to traverse that network element. IPsec will usually lower its tunnel MTU when a path MTU message is received.
Protocol failures	The number of malformed IPsec packets that have been received.
Missing SA failures	The number of IPsec operations that have been requested for which the specified IPsec security association does not exist.
System capacity failures	The number of IPsec operations that cannot be completed because the capacity of the IPsec system is not high enough to support the data rate.

Examples

The following example, entered in global configuration mode, displays IPsec statistics:

```
ciscoasa(config)# show ipsec stats
IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
 Fragmentation successes: 3
  Pre-fragmentation successes:2
  Post-fragmentation successes: 1
 Fragmentation failures: 2
  Pre-fragmentation failures:1
  Post-fragmentation failures: 1
 Fragments created: 10
 PMTUs sent: 1
 PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
```

On platforms that support IPsec flow offload, the output shows the counters for offloaded flows, and the regular counters show the total of offloaded and non-offloaded flows.

```
ciscoasa# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 1
Previous tunnels: 1
Inbound
    Bytes: 93568
    Decompressed bytes: 0
    Packets: 86
    Dropped packets: 0
    Replay failures: 0
    Authentications: 0
    Authentication failures: 0
    Decryptions: 86
    Decryption failures: 0
    TFC Packets: 0
    Decapsulated fragments needing reassembly: 0
    Valid ICMP Errors rcvd: 0
    Invalid ICMP Errors rcvd: 0
Outbound
    Bytes: 93568
    Uncompressed bytes: 90472
    Packets: 86
    Dropped packets: 0
    Authentications: 0
    Authentication failures: 0
    Encryptions: 86
    Encryption failures: 0
    TFC Packets: 0
    Fragmentation successes: 0
        Pre-fragmentation successes: 0
        Post-fragmentation successes: 0
    Fragmentation failures: 0
        Pre-fragmentation failures: 0
        Post-fragmentation failures: 0
    Fragments created: 0
    PMTUs sent: 0
    PMTUs rcvd: 0
Offloaded Inbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Decryptions: 86
Offloaded Outbound
    Bytes: 93568
    Packets: 86
    Authentications: 0
    Encryptions: 86
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
Inbound SA delete requests: 0
Outbound SA delete requests: 0
Inbound SA destroy calls: 0
Outbound SA destroy calls: 0
```

Related Commands

Command	Description
clear ipsec sa	Clears IPsec SAs or counters based on specified parameters.
crypto ipsec transform-set	Defines a transform set.
show ipsec sa	Displays IPsec SAs based on specified parameters.
show ipsec sa summary	Displays a summary of IPsec SAs.

show ipv – show ir

show ipv6 access-list

To display the IPv6 access list, use the **show ipv6 access-list** command in privileged EXEC mode. The IPv6 access list determines what IPv6 traffic can pass through the ASA.

show ipv6 access-list [*id* [*source-ipv6-prefix/prefix-length* **| any | host** *source-ipv6-address*]]

Syntax Description

any	(Optional) An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	(Optional) IPv6 address of a specific host. When provided, only the access rules for the specified host are displayed.
id	(Optional) The access list name. When provided, only the specified access list is displayed.
source-ipv6-prefix /prefix-length	(Optional) IPv6 network address and prefix. When provided, only the access rules for the specified IPv6 network are displayed.

Command Default

Displays all IPv6 access lists.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	IPv6 access rules were incorporated into the **access-list** command, so this command is no longer meaningful.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

This command shows only those access lists configured using the **ipv6 access-list** command. In ASA 9.0(1), IPv6 access control was integrated into the same **access-list** structure as IPv4. Thus, in systems running software versions starting with 9.0(1), the **show ipv6 access-list** command is no longer meaningful.

Examples

The following is sample output from the **show ipv6 access-list** command. It shows IPv6 access lists named inbound, tcptraffic, and outbound.

```
ciscoasa# show ipv6 access-list
```

```
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

Related Commands

Command	Description
ipv6 access-list	Creates an IPv6 access list.

show ipv6 dhcp

To show DHCPv6 information, use the **show ipv6 dhcp** command in privileged EXEC mode.

show ipv6 dhcp [**client** [**pd**] **statistics | interface** [*interface_name* [**statistics**]] **| ha statistics | server statistics | pool** [*pool_name*]]

Syntax Description

client	Shows DHCPv6 client statistics and shows the output of the number of messages sent and received.
pd	Shows DHCPv6 Prefix Delegation client statistics.
statistics	Shows statistics.
interface	Shows DHCPv6 information for all interfaces. If the interface is configured for DHCPv6 stateless server configuration (see **ipv6 dhcp server**), this command lists the DHCPv6 pool that is being used by the server. If the interface has DHCPv6 address client or Prefix Delegation client configuration, this command shows the state of each client and the values received from the server.
interface_name	(Optional) For a specific interface, you can show message statistics for the DHCP server or client.
ha	Shows the transaction statistics between failover units, including how many times the DUID information was synced between the units.
server	Shows the DHCPv6 stateless server statistics.
pool	Shows DHCPv6 pools.
pool_name	(Optional) Shows the specified pool.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

If you do not specify any arguments, this command displays the device DUID that is being used by the DHCPv6 client or server.

Examples

The following is sample output from the **show ipv6 dhcp** command:

```
ciscoasa# show ipv6 dhcp
This device's DHCPv6 unique identifier(DUID): 00030001377E8FD91020
```

The following is sample output from the **show ipv6 dhcp pool** command:

```
ciscoasa# show ipv6 dhcp pool
DHCPv6 pool: Sample-Pool
  Imported DNS server: 2004:abcd:abcd:abcd::2
  Imported DNS server: 2004:abcd:abcd:abcd::4
  Imported Domain name: relay.com
  Imported Domain name: server.com
  SIP server address: 2001::abcd:1
  SIP server domain name: sip.xyz.com
```

The following is sample output from the **show ipv6 dhcp interface** command:

```
ciscoasa# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool
GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD
Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0
```

The following is sample output from the **show ipv6 dhcp interface outside** command:

```
ciscoasa# show ipv6 dhcp interface outside
GigabitEthernet1/2 is in client mode
 Prefix State is OPEN
 Renew will be sent in 00:02:05
 Address State is OPEN
 Renew for address will be sent in 00:02:06
 List of known servers:
   Reachable via address: fe80::20c:29ff:fe96:1bf4
   DUID: 000100011D9D1712005056A07E06
   Preference: 0
   Configuration parameters:
     IA PD: IA ID 0x00030001, T1 250, T2 400
       Prefix: 2005:abcd:ab03::/48
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     IA NA: IA ID 0x00030001, T1 250, T2 400
       Address: 2004:abcd:abcd:abcd:abcd:abcd:f2cb/128
               preferred lifetime 500, valid lifetime 600
               expires at Nov 26 2014 03:11 PM (476 seconds)
     DNS server: 2004:abcd:abcd:abcd::2
     DNS server: 2004:abcd:abcd:abcd::4
     Domain name: relay.com
     Domain name: server.com
     Information refresh time: 0
 Prefix name: Sample-PD
```

The following is sample output from the **show ipv6 dhcp interface outside statistics** command:

```
ciscoasa# show ipv6 dhcp interface outside statistics
DHCPV6 Client PD statistics:
Protocol Exchange Statistics:
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0
Error and Failure Statistics:
 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
DHCPV6 Client address statistics:
Protocol Exchange Statistics:
 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0
Error and Failure Statistics:
 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp client statistics** command:

```
ciscoasa# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:               92
  Total number of Rebind messages sent:              0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0
Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp client pd statistics** command:

```
ciscoasa# show ipv6 dhcp client pd statistics
Protocol Exchange Statistics:
 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0
Error and Failure Statistics:
 Total number of Re-transmission messages sent:                  1
 Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp server statistics** command:

```
ciscoasa# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:            0
  Total number of Advertise messages sent:              0
  Total number of Request messages received:            0
  Total number of Renew messages received:              0
  Total number of Rebind messages received:             0
  Total number of Reply messages sent:                  10
  Total number of Release messages received:            0
  Total number of Reconfigure messages sent:            0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:      0
  Total number of Relay-Reply messages sent:            0
Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

The following is sample output from the **show ipv6 dhcp ha statistics** command:

```
ciscoasa# show ipv6 dhcp ha statistics
DHCPv6 HA global statistics:
  DUID sync messages sent:             1
  DUID sync messages received:         0
```

```
DHCPv6 HA error statistics:
  Send errors:                         0
```

The following is sample output from the **show ipv6 dhcp ha statistics** command on a standby unit:

```
ciscoasa# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:             0
  DUID sync messages received:         1
DHCPv6 HA error statistics:
  Send errors:                         0
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

show ipv6 dhcprelay binding

To display the relay binding entries created by the relay agent, use the **show ipv6 dhcprelay binding** command in privileged EXEC mode.

show ipv6 dhcprelay binding

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 dhcprelay binding** command allows you to check the relay binding entries that the relay agent has created.

Examples

The following is sample output from the **show ipv6 dhcprelay binding** command:

```
ciscoasa# show ipv6 dhcprelay binding
1 in use, 2 most used
Client: fe80::204:23ff:febb:b094 (inside)
  DUID: 000100010f9a59d1000423bbb094, Timeout in 60 seconds
Above binding is created for client with link local address of fe80::204:23ff:febb:b094 on
 the inside interface using DHCPv6 id of 000100010f9a59d1000423bbb094, and will timeout in
 60 seconds.
There will be limit of 1000 bindings for each context.
```

Related Commands

Command	Description
show ipv6 dhcprelay statistics	Shows the IPv6 DHCP relay agent information.

show ipv6 dhcprelay statistics

To display the IPv6 DHCP relay agent statistics, use the **show ipv6 dhcprelay statistics** command in privileged EXEC mode.

show ipv6 dhcprelay statistics

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 dhcprelay statistics** command allows you to view IPv6 DHCP relay agent information.

Examples

The following is sample output from the **show ipv6 dhcprelay statistics** command:

```
ciscoasa# show ipv6 dhcprelay statistics
Relay Messages:
  SOLICIT                                         1
  ADVERTISE                                       2
  REQUEST                                         1
  CONFIRM                                         1
  RENEW                                         496
  REBIND                                          0
  REPLY                                         498
  RELEASE                                         0
  DECLINE                                         0
  RECONFIGURE                                     0
  INFORMATION-REQUEST                             0
  RELAY-FORWARD                                 499
  RELAY-REPLY                                   500
Relay Errors:
  Malformed message:                              0
  Block allocation/duplication failures:          0
  Hop count limit exceeded:                       0
  Forward binding creation failures:              0
  Reply binding lookup failures:                  0
  No output route:                                0
  Conflict relay server route:                    0
  Failed to add server NP rule:                0
  Unit or context is not active:               0
Total Relay Bindings Created:                498
```

Related Commands

Command	Description
show ipv6 dhcprelay binding	Shows the relay binding entries created by the relay agent.

show ipv6 general-prefix

To show all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes, use the **show ipv6 general-prefix** command in privileged EXEC mode.

show ipv6 general-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

To see the preferred lifetime of the prefix assigned by the DHCPv6 Server, use the **show ipv6 general-prefix** command. When you use Prefix Delegation, you must set the ASA IPv6 neighbor discovery router advertisement interval to be much lower than the preferred lifetime of the prefix assigned by the DHCPv6 Server to prevent IPv6 traffic interruption. For example, if the DHCPv6 server sets the preferred Prefix Delegation lifetime to 300 seconds, you should set the ASA RA interval to be 150 seconds. To set the ASA RA interval, see the **ipv6 nd ra-interval** command; the default is 200 seconds.

Examples

The following is sample output from the **show ipv6 general-prefix** command that shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes ("Consumer List"):

```
ciscoasa# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
    BGP network command         1
    inside (Address command)    1
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.

Command	Description
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

show ipv6 icmp

To display the ICMPv6 access rules configured on all interfaces, use the **show ipv6 icmp** command in privileged EXEC mode.

show ipv6 icmp

Syntax Description

This command has no arguments or variables.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

ICMPv6 rules control ICMPv6 traffic to device interfaces. They do not control through-the-box traffic. You would use these rules to control which addresses could send ICMPv6 commands to an interface (for example, pings), and which types of ICMPv6 commands could be sent. Use the **show ipv6 icmp** command to view these rules.

Examples

The following is sample output from the **show ipv6 icmp** command.

```
ciscoasa show ipv6 icmp
ipv6 icmp permit any inside
```

Related Commands

Command	Description
ipv6 icmp	Configures IPv6 ICMP management access rules.

show ipv6 interface

To display the status of interfaces configured for IPv6, use the **show ipv6 interface** command in privileged EXEC mode.

show ipv6 interface [**brief**] [*if_name* [**prefix**]]

Syntax Description

brief	Displays a brief summary of IPv6 status and configuration for each interface.
if_name	(Optional) The internal or external interface name, as designated by the **nameif** command. The status and configuration for only the designated interface is shown.
prefix	(Optional) Prefix generated from a local IPv6 prefix pool. The prefix is the network portion of the IPv6 address.

Command Default

Displays all IPv6 interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.10(1)	For the Firepower 2100/4100/9300, the output of the command is enhanced to indicate the supervisor association status of the interfaces.
9.10(1)	Support to indicate supervisor non-association for the Firepower 2100/4100/9300 was added.

Usage Guidelines

The **show ipv6 interface** command provides output similar to the **show interface** command, except that it is IPv6-specific. If the interface hardware is usable, the interface is marked >*up* . If the interface can provide two-way communication, the line protocol is marked >*up* . For Firepower 2100/4100/9300 devices, to indicate supervisor is not associated with IPv6 interfaces, “not associated with Supervisor” is displayed along the line protocol status.

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 interface** command:

```
ciscoasa# show ipv6 interface outside
```

```
interface ethernet0 “outside” is up, line protocol is up “not associated with Supervisor”
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

The following is sample output from the **show ipv6 interface** command when entered with the **brief** keyword:

```
ciscoasa# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

For Firepower 2100/4100/9300 devices, to indicate supervisor is not associated with IPv6 interfaces, “not associated with Supervisor” is displayed along the line protocol status. The following is sample output from the **show ipv6 interface** command. It shows the characteristics of an interface which has generated a prefix from an address.

```
ciscoasa# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar
AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 local pool

To display IPv6 address pool information, use the **show ipv6 local pool** command in privileged EXEC mode.

show ipv6 local pool interface *pool_name*

Syntax Description

pool_name	The name of the address pool. Enter ? to see a list of pools.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

Use this command to view the contents of IPv6 address pools created using the **ipv6 local pool** command. These pools are used with remote access VPN and clustering. Use the **ip local pool** command to view IPv4 address pools.

Examples

The following is sample output from the **show ipv6 local pool** command:

```
ciscoasa# show ipv6 local pool test-ipv6-pool

IPv6 Pool test-ipv6-pool
Begin Address: 2001:db8::db8:800:200c:417a
End Address: 2001:db8::db8:800:200c:4188
Prefix Length: 64
Pool Size: 15
Number of used addresses: 0
Number of available addresses: 15
Available Addresses:
2001:db8::db8:800:200c:417a
2001:db8::db8:800:200c:417b
2001:db8::db8:800:200c:417c
2001:db8::db8:800:200c:417d
2001:db8::db8:800:200c:417e
2001:db8::db8:800:200c:417f
2001:db8::db8:800:200c:4180
2001:db8::db8:800:200c:4181
2001:db8::db8:800:200c:4182
2001:db8::db8:800:200c:4183
2001:db8::db8:800:200c:4184
2001:db8::db8:800:200c:4185
2001:db8::db8:800:200c:4186
```

```
2001:db8::db8:800:200c:4187
2001:db8::db8:800:200c:4188
```

Related Commands

Command	Description
ipv6 local pool	Configures an IPv6 address pool.

show ipv6 mld traffic

To display the Multicast Listener Discovery (MLD) traffic counter information, use the **show ipv6 mld traffic** command in privileged EXEC mode.

show ipv6 mld traffic

Syntax Description

This command has no keywords or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)	This command was added.

Usage Guidelines

The **show ipv6 mld traffic** command allows you to check if the expected number of MLD messages have been received and sent.

The following information is provided by the **show ipv6 mld traffic** command:

- Elapsed time since counters cleared—The amount of time since the counters were cleared.
- Valid MLD Packets—The number of valid MLD packets that are received and sent.
- Queries—The number of valid queries that are received and sent.
- Reports—The number of valid reports that are received and sent.
- Leaves—The number of valid leaves received and sent.
- Mtraee packets—The number of multicast trace packets that are received and sent.
- Errors—The types of errors and the number of errors that have occurred.

Examples

The following is sample output from the **show ipv6 mld traffic** command:

```
ciscoasa# show ipv6 mld traffic
show ipv6 mld traffic
MLD Traffic Counters
Elapsed time since counters cleared: 00:01:19
     Received      Sent
```

```
Valid MLD Packets      1      3
Queries      1      0
Reports       0      3
Leaves      0      0
Mtrace packets      0     0
Errors:
Malformed Packets      0
Martian source      0
Non link-local source 0
Hop limit is not equal to 1 0
```

Related Commands

Command	Description
clear ipv6 mld traffic	Resets all MLD traffic counters.

show ipv6 neighbor

To display the IPv6 neighbor discovery cache information, use the **show ipv6 neighbor** command in privileged EXEC mode.

show ipv6 neighbor [*if_name* | *address*]

Syntax Description

address	(Optional) Displays neighbor discovery cache information for the supplied IPv6 address only.
if_name	(Optional) Displays cache information for the supplied interface name, as configured by the **nameif** command only.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The following information is provided by the **show ipv6 neighbor** command:

- IPv6 Address—The IPv6 address of the neighbor or interface.
- Age—The time (in minutes) since the address was confirmed to be reachable. A hyphen (-) indicates a static entry.
- Link-layer Addr—The MAC address. If the address is unknown, a hyphen (-) is displayed.
- State—The state of the neighbor cache entry.

Note Reachability detection is not applied to static entries in the IPv6 neighbor discovery cache; therefore, the descriptions for the INCMP (Incomplete) and REACH (Reachable) states are different for dynamic and static cache entries.

The following are possible states for dynamic entries in the IPv6 neighbor discovery cache:

- INCMP—(Incomplete) Address resolution is being performed on the entry. A neighbor solicitation message has been sent to the solicited-node multicast address of the target, but the corresponding neighbor advertisement message has not yet been received.

- REACH—(Reachable) Positive confirmation was received within the last ReachableTime milliseconds that the forward path to the neighbor was functioning properly. While in REACH state, the device takes no special action as packets are sent.
- STALE—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. While in STALE state, the device takes no action until a packet is sent.
- DELAY—More than ReachableTime milliseconds have elapsed since the last positive confirmation was received that the forward path was functioning properly. A packet was sent within the last DELAY_FIRST_PROBE_TIME seconds. If no reachability confirmation is received within DELAY_FIRST_PROBE_TIME seconds of entering the DELAY state, send a neighbor solicitation message and change the state to PROBE.
- PROBE—A reachability confirmation is actively sought by resending neighbor solicitation messages every RetransTimer milliseconds until a reachability confirmation is received.
- ????—Unknown state.

The following are possible states for static entries in the IPv6 neighbor discovery cache:

- INCMP—(Incomplete) The interface for this entry is down.
- REACH—(Reachable) The interface for this entry is up.

- Interface

The interface from which the address was reachable.

Examples

The following is sample output from the **show ipv6 neighbor** command when entered with an interface:

```
ciscoasa# show ipv6 neighbor inside
IPv6 Address                             Age Link-layer Addr State Interface
2000:0:0:4::2                              0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                   0 0003.a0d6.141e  REACH inside
3001:1::45a                                - 0002.7d1a.9472  REACH inside
```

The following is sample output from the **show ipv6 neighbor** command when entered with an IPv6 address:

```
ciscoasa# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                             Age Link-layer Addr State Interface
2000:0:0:4::2                              0 0003.a0d6.141e  REACH inside
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
ipv6 neighbor	Configures a static entry in the IPv6 neighbor discovery cache.

show ipv6 ospf

To display general information about OSPFv3 routing processes, use the **show ipv6 ospf** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*]

Syntax Description

area_id	(Optional) Shows information about a specified area only.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 ospf** command lists the following settings:

- Event logging
- Router type
- Redistribution route type
- SPF schedule delay
- Hold time between two consecutive SPFs
- Wait time between two consecutive SPFs
- Minimum LSA interval
- Minimum LSA arrival

Examples

The following is sample output from the **show ipv6 ospf** command:

```
ciscoasa# show ipv6 ospf
Routing Process “ospfv3 1” with ID 10.9.4.1
Event-log enabled, Maximum number of events: 1000, Mode: cyclic
It is an autonomous system boundary router
Redistributing External Routes from,
   ospf 2
Initial SPF schedule delay 5000 msecs
Minimum hold time between two consecutive SPFs 10000 msecs
Maximum wait time between two consecutive SPFs 10000 msecs
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msecs
```

Related Commands

Command	Description
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).
show ipv6 ospf database	Shows lists of information related to the OSPFv3 database for a specific router.

show ipv6 ospf border-routers

To display the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR), use the **show ipv6 ospf border-routers** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **border-routers**

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show ipv6 ospf border-routers** command lists the following settings:

- Intra-area route
- Inter-area route
- IPv6 address
- Interface type
- Area ID
- SPF number

Examples

The following is sample output from the **show ipv6 ospf border-routers** command:

```
ciscoasa# show ipv6 ospf border-routers
OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 172.16.4.4 [2] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ABR, Area 1, SPF 13
```

```
i 172.16.4.4 [1] via FE80::205:5FFF:FED3:5406, POS4/0, ABR, Area 0, SPF 8
i 172.16.3.3 [1] via FE80::205:5FFF:FED3:5808, FastEthernet0/0, ASBR, Area 1, SPF 3
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf database	Shows lists of information related to the OSPFv3 database for a specific router.

show ipv6 ospf database

To display lists of information related to the OSPFv3 database for a specific router, use the **show ipv6 ospf database** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **database** [**external | inter-area prefix | inter-area-router | network | nssa-external | router | area | as | ref-lsa** [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] **| self-originate**] [**internal**] [**database-summary**]

Syntax Description

adv-router *router-id*	(Optional) Displays all the LSAs of the advertising router. The router ID must be in the form documented in RFC 2740, in which the address is specified in hexadecimal using 16-bit values between colons.
area	(Optional) Displays information only about area LSAs.
area_id	(Optional) Displays information about a specified area only.
as	(Optional) Filters unknown autonomous system (AS) LSAs.
database-summary	(Optional) Displays how many of each type of LSA exists for each area in the database and the total.
destination-router-id	(Optional) Displays information about a specified destination router only.
external	(Optional) Displays information only about the external LSAs.
interface	Optional) Displays information about the LSAs filtered by interface context.
interface-name	(Optional) Specifies the LSA interface name.
internal	(Optional) Displays information only about the internal LSAs.
inter-area prefix	(Optional) Displays information only about LSAs based on inter-area prefix.
inter-area router	(Optional) Displays information only about LSAs based on inter-area router LSAs.
link	(Optional) Displays information about link LSAs. When it follows the **unknown** keyword, the **link** keyword filters link-scope LSAs.
link-state-id	(Optional) Specifies an integer used to differentiate LSAs. In network and link LSAs, the link-state ID matches the interface index.
network	(Optional) Displays information about network LSAs.
nssa-external	(Optional) Displays information only about the not so stubby area (NSSA) external LSAs.
prefix *ipv6-prefix*	(Optional) Displays the link-local IPv6 address of the neighbor. The IPv6 prefix must be in the form documented in RFC 2373, in which the address is specified in hexadecimal using 16-bit values between colons.

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
ref-lsa	(Optional) Further filters the prefix LSA type.
router	(Optional) Displays information about router LSAs.
self-originate	(Optional) Displays only self-originated LSAs from the local router.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The various forms of the command provide information about different OSPFv3 LSAs.

Examples

The following is sample output from the **show ipv6 ospf database** command:

```
ciscoasa# show ipv6 ospf database
            OSPFv3 Router with ID (172.16.4.4) (Process ID 1)
                Router Link States (Area 0)
ADV Router         Age         Seq#        Fragment ID   Link count  Bits
172.16.4.4         239         0x80000003  0             1           B
172.16.6.6         239         0x80000003  0             1           B
            Inter Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Prefix
172.16.4.4         249         0x80000001  FEC0:3344::/32
172.16.4.4         219         0x80000001  FEC0:3366::/32
172.16.6.6         247         0x80000001  FEC0:3366::/32
172.16.6.6         193         0x80000001  FEC0:3344::/32
172.16.6.6         82          0x80000001  FEC0::/32
            Inter Area Router Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Dest RtrID
172.16.4.4         219         0x80000001  50529027   172.16.3.3
172.16.6.6         193         0x80000001  50529027   172.16.3.3
            Link (Type-8) Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Interface
172.16.4.4         242         0x80000002  14         PO4/0
172.16.6.6         252         0x80000002  14         PO4/0
```

```
            Intra Area Prefix Link States (Area 0)
ADV Router         Age         Seq#        Link ID    Ref-lstype  Ref-LSID
172.16.4.4         242         0x80000002  0          0x2001      0
172.16.6.6         252         0x80000002  0          0x2001      0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf events

To display OSPFv3 internal event information, use the **show ipv6 ospf events** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **events** [*type*]

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type	(Optional) A list of the event types you want to see. If you do not specify one or more types, you see all events. You can filter on the following types: • **generic**—Generic events. • **interface**—Interface state change events. • **lsa**—LSA arrival and LSA generation events. • **neighbor**—Neighbor state change events. • **reverse**—Show events in reverse order. • **rib**—Router Information Base update, delete and redistribution events. • **spf**—SPF scheduling and SPF run events.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Examples

The following is sample output from the **show ipv6 ospf events** command:

```
ciscoasa# show ipv6 ospf events
OSPFv3 Router with ID (10.1.3.2) (Process ID 10)
```

```
  1 Jul 9  18:49:34.071: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
  2 Jul 9  18:49:31.571: Rcv Unchanged Type-0x2001 LSA, LSID 0.0.0.0, Adv-Rtr 10.1.1.2,
 Seq# 80000008, Age 1, Area 10
  3 Jul 9  18:48:13.241: Generate Changed Type-0x8 LSA, LSID 2.0.0.0, Seq# 80000004, Age
  0, Area 10
  4 Jul 9  18:48:13.241: Generate Changed Type-0x2001 LSA, LSID 0.0.0.0, Seq# 80000005,
 Age 0, Area 10
  5 Jul 9  18:41:18.901: End of SPF, SPF time 0ms, next wait-interval 10000ms
  6 Jul 9  18:41:18.902: Starting External processing in area 10
  7 Jul 9  18:41:18.902: Starting External processing
  8 Jul 9  18:41:18.902: Starting Inter-Area SPF in area 10
  9 Jul 9  18:41:18.902: Generic:  post_spf_intra  0x0
 10 Jul 9  18:41:18.902: RIB Delete (All Paths), Prefix 2002::/64, type Intra
 11 Jul 9  18:41:18.902: RIB Update, Prefix 5005::/64, gw ::, via inside, type Intra
 12 Jul 9  18:41:18.902: Starting Intra-Area SPF in Area 10
 13 Jul 9  18:41:18.903: Starting SPF, wait-interval 5000ms
 14 Jul 9  18:41:16.403: Timer Exp:  ospfv3_if_ack_delayed  0xda05fad8
 15 Jul 9  18:41:13.903: Schedule SPF, Area 10, Change in LSA type PLSID 0.8.0.0, Adv-Rtr
  50.100.168.192
 16 Jul 9  18:41:13.903: Rcv Changed Type-0x2009 LSA, LSID 0.8.0.0, Adv-Rtr 10.1.2.3,
Seq# 80000003, Age 1, Area 10
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf flood-list

To display a list of OSPFv3 LSAs waiting to be flooded over an interface, use the **show ipv6 ospf flood-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **flood-list** *interface-type interface-number*

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface-number	Specifies the interface number over which the LSAs are flooded.
interface-type	Specifies the interface type over which the LSAs are flooded.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPFv3 routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to display OSPFv3 packet pacing information.

Examples

The following is sample output from the **show ipv6 ospf flood-list** command:

```
ciscoasa# show ipv6 ospf flood-list
OSPFv3 Router with ID (172.16.6.6) (Process ID 1)
 Interface POS4/0, Queue length 1
 Link state retransmission due in 14 msec
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               172.16.6.6      0x80000031  0      0x1971
 Interface FastEthernet0/0, Queue length 0
 Interface ATM3/0, Queue length 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf graceful-restart

To display information about OSPFv3 graceful-restart, use the **show ipv6 ospf** graceful-restart command in privileged EXEC mode.

show ipv6 ospf graceful-restart

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Examples

The following is sample output from the **show ipv6 ospf graceful-restart** command:

```
ciscoasa# show ipv6 ospf graceful-restart
Routing Process "ospfv3 10"
  Graceful Restart enabled
    restart-interval limit: 240 sec
    Clustering is not configured in spanned etherchannel mode
  Graceful Restart helper support enabled
    Number of neighbors performing Graceful Restart is 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.

show ipv6 ospf interface

To display OSPFv3-related interface information, use the **show ipv6 ospf interface** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **interface** [*type-number*] [**brief**]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
brief	(Optional) Displays brief overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type-number	(Optional) Specifies the interface type and number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to display overview information for OSPFv3 interfaces, states, addresses and masks, and areas on the router.

Examples

The following is sample output from the **show ipv6 ospf interface** command:

```
ciscoasa# show ipv6 ospf interface
ATM3/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 13
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type POINT_TO_POINT, Cost: 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
  Index 1/2/2, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.4.4
  Suppress hello for 0 neighbor(s)
FastEthernet0/0 is up, line protocol is up
  Link Local Address 2001:0DB1:205:5FFF:FED3:5808, Interface ID 3
  Area 1, Process ID 1, Instance ID 0, Router ID 172.16.3.3
  Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State BDR, Priority 1
  Designated Router (ID) 172.16.6.6, local address 2001:0DB1:205:5FFF:FED3:6408
  Backup Designated router (ID) 172.16.3.3, local address 2001:0DB1:205:5FFF:FED3:5808
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1/1, flood queue length 0
  Next 0x0(0)/0x0(0)/0x0(0)
  Last flood scan length is 12, maximum is 12
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 172.16.6.6  (Designated Router)
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf neighbor

To display OSPFv3 neighbor information on a per-interface basis, use the **show ipv6 ospf neighbor** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **neighbor** [*interface-type interface-number*] [*neighbor-id*] [**detail**]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
detail	(Optional) Displays all neighbors information in detail.
interface-type interface-number	(Optional) Specifies the interface type and number.
neighbor-id	(Optional) Specifies the neighbor ID.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to display detailed information for OSPFv3 neighbors by interface.

Examples

The following is sample output from the **show ipv6 ospf neighbor** command:

```
ciscoasa# show ipv6 ospf neighbor
Neighbor ID     Pri   State           Dead Time   Interface ID    Interface
172.16.4.4       1    FULL/  -        00:00:31    14              POS4/0
172.16.3.3       1    FULL/BDR        00:00:30    3               FastEthernet00
172.16.5.5       1    FULL/  -        00:00:33    13              ATM3/0
```

The following is sample output from the **show ipv6 ospf neighbor detail** command:

```
Neighbor 172.16.4.4
    In the area 0 via interface POS4/0
    Neighbor: interface-id 14, link-local address FE80::205:5FFF:FED3:5406
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63AD1B0D
    Dead timer due in 00:00:33
    Neighbor is up for 00:48:56
    Index 1/1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.3.3
    In the area 1 via interface FastEthernet0/0
    Neighbor: interface-id 3, link-local address FE80::205:5FFF:FED3:5808
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 172.16.6.6 BDR is 172.16.3.3
    Options is 0x63F813E9
    Dead timer due in 00:00:33
    Neighbor is up for 00:09:00
    Index 1/1/2, retransmission queue length 0, number of retransmission 2
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 2
    Last retransmission scan time is 0 msec, maximum is 0 msec
 Neighbor 172.16.5.5
    In the area 2 via interface ATM3/0
    Neighbor: interface-id 13, link-local address FE80::205:5FFF:FED3:6006
    Neighbor priority is 1, State is FULL, 6 state changes
    Options is 0x63F7D249
    Dead timer due in 00:00:38
    Neighbor is up for 00:10:01
    Index 1/1/3, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0)/0x0(0) Next 0x0(0)/0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf request-list

To display a list of all LSAs that have been requested by a router, use the **show ipv6 ospf request-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface	(Optional) Specifies the list of all LSAs requested by the router from this interface.
interface-neighbor	(Optional) Specifies the list of all LSAs requested by the router on this interface from this neighbor.
neighbor	(Optional) Specifies the list of all LSAs requested by the router from this neighbor.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to list all LSAs that a router requests.

Examples

The following is sample output from the **show ipv6 ospf request-list** command:

```
ciscoasa# show ipv6 ospf request-list
            OSPFv3 Router with ID (192.168.255.5) (Process ID 1)
 Neighbor 192.168.255.2, interface Ethernet0/0 address
FE80::A8BB:CCFF:FE00:6600
 Type    LS ID          ADV RTR         Seq NO      Age    Checksum
  1      0.0.0.0        192.168.255.3   0x800000C2  1      0x0014C5
  1      0.0.0.0        192.168.255.2   0x800000C8  0      0x000BCA
  1      0.0.0.0        192.168.255.1   0x800000C5  1      0x008CD1
  2      0.0.0.3         192.168.255.3   0x800000A9  774     0x0058C0
  2      0.0.0.2         192.168.255.3   0x800000B7  1       0x003A63
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf retransmission-list

To display a list of all LSAs that have been waiting to be resent, use the **show ipv6 ospf retransmission-list** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] [*area_id*] **retransmission-list** [*neighbor*] [*interface*] [*interface-neighbor*]

Syntax Description

area_id	(Optional) Displays information about a specified area only.
interface	(Optional) Specifies the list of all LSAs waiting to be resent on this interface.
interface-neighbor	(Optional) Specifies the list of all LSAs waiting to be resent for this interface from this neighbor.
neighbor	(Optional) Specifies the list of all LSAs waiting to be resent for this neighbor.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to list all LSAs that are waiting to be resent.

Examples

The following is sample output from the **show ipv6 ospf retransmission-list** command:

```
ciscoasa# show ipv6 ospf retransmission-list
        OSPFv3 Router with ID (192.168.255.2) (Process ID 1)
 Neighbor 192.168.255.1, interface Ethernet0/0
 Link state retransmission due in 3759 msec, Queue length 1
 Type    LS ID           ADV RTR         Seq NO      Age    Checksum
 0x2001  0               192.168.255.2   0x80000222  1      0x00AE52
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf statistic

To display various OSPFv3 statistics, use the **show ipv6 ospf statistic** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **statistic** [**detail**]

Syntax Description

detail	(Optional) Specifies detailed SPF information, including the trigger points.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to list the number of times SPF was executed, the reasons, and the duration.

Examples

The following is sample output from the **show ipv6 ospf statistic** command:

```
ciscoasa# show ipv6 ospf 10 statistic detail
Area 10: SPF algorithm executed 6 times
SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
             0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)
SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
```

```
SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
     0      0      0      0      0      0      0 0
RIB manipulation time (in msec):
RIB Update    RIB Delete
             0             0
LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
Change record R N L
LSAs changed 5
Changed LSAs. Recorded is Advertising Router, LSID and LS type:
50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
50.100.168.192/2(N)
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf summary-prefix

To display a list of all summary address redistribution information configured under an OSPFv3 process, use the **show ipv6 ospf summary-prefix** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **summary-prefix**

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show a list of all summary address redistribution information that has been configured under an OSPFv3 process.

Examples

The following is sample output from the **show ipv6 ospf summary-prefix** command:

```
ciscoasa# show ipv6 ospf summary-prefix
OSPFv3 Process 1, Summary-prefix
FEC0::/24 Metric 16777215, Type 0, Tag 0
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf timers

To display OSPFv3 timers information, use the **show ipv6 ospf timers** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **timers** [**lsa-group** | **rate-limit**]

Syntax Description

lsa-group	(Optional) Specifies OSPFv3 LSA group information.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
rate-limit	(Optional) Specifies OSPFv3 LSA rate limit information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show LSA information that has been configured under an OSPFv3 process.

Examples

The following is sample output from the **show ipv6 ospf timers lsa-group** command:

```
ciscoasa# show ipv6 ospf timers lsa-group
OSPFv3 Router with ID (10.10.13.101) (Process ID 1)
Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:13
Current time 96532
Index 0 Timestamp 96546
Index 1 Timestamp 96788
Index 2 Timestamp 97048
Index 3 Timestamp 97293
Index 4 Timestamp 97548
Failure Head 0, Last 0 LSA group failure logged
            OSPFv3 Router with ID (10.10.10.102) (Process ID 5709)
Group size 5, Head 2, Search Index 4, Interval 240 sec
Next update due in 0:00:22
```

```
Current time 96532
Index 0 Timestamp 96555
Index 1 Timestamp 96801
Index 2 Timestamp 97041
Index 3 Timestamp 97287
Index 4 Timestamp 97546
Failure Head 0, Last 0 LSA group failure logged
```

The following is sample output from the **show ipv6 ospf timers rate-limit** command:

```
ciscoasa# show ipv6 ospf timers rate-limit
List of LSAs that are in rate limit Queue
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf traffic

To display OSPFv3 traffic-related statistics for currently available interfaces, use the **show ipv6 ospf traffic** command in user EXEC or privileged EXEC mode.

show ipv6 ospf [*process_id*] **traffic** [*interface_name*]

Syntax Description

interface_name	(Optional) Specifies the name of the interface (for example, interface GigabitEthernet0/0). Use this option to segregate traffic to a specific interface.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show OSPFv3 traffic-related information for available interfaces.

Examples

The following is sample output from the **show ipv6 ospf traffic** command:

```
ciscoasa# show ipv6 ospf 10 traffic inside
Interface inside
Last clearing of interface traffic counters never
OSPFv3 packets received/sent
  Type          Packets              Bytes
  RX Invalid                       0 0
  RX Hello                      1232 53132
  RX DB des                       27 896
  RX LS req                        3 216
  RX LS upd                       28 2436
  RX LS ack                       14 1064
  RX Total                      1304 57744
  TX Failed                        0 0
  TX Hello                       753 32072
  TX DB des                       27 1056
  TX LS req                      2 92
  TX LS upd                      9 1128
  TX LS ack                     15 900
  TX Total                     806 35248
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 ospf virtual-links

To displayparameters and the current state of OSPFv3 virtual links, use the **show ipv6 ospf virtual-links** command in user EXEC or privileged EXEC mode.

show ipv6 ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to show parameters and the current state of OSPFv3 virtual links.

Examples

The following is sample output from the **show ipv6 ospf virtual-links** command:

```
ciscoasa# show ipv6 ospf virtual-links
Virtual Link OSPF_VL0 to router 172.16.6.6 is up
  Interface ID 27, IPv6 address FEC0:6666:6666::
  Run as demand circuit
  DoNotAge LSA allowed.
  Transit area 2, via interface ATM3/0, Cost of using 1
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:06
```

Related Commands

Command	Description
show ipv6 ospf	Shows all IPv6 settings in the OSPFv3 routing process.
show ipv6 ospf border-routers	Shows the internal OSPFv3 routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ipv6 prefix-list

To display information about configured IPv6 prefix lists, use the **show ipv6 prefix-list** command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [**summary | detail**] [*policy list_name* [**seq** *sequence_number* | *network/length* [**longer | first-match**]]]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.
summary	(Optional) Show additional summarized statistical information.
detail	(Optional) Show additional summarized statistical information plus prefix list entries.
seq *sequence_number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
network/length [**longer** | **first-match**]	(Optional) Displays all entries in the specified prefix list that use this network address and prefix length (in bits). You can add these keywords to modify the match: • **longer**—Displays all entries of the specified prefix list that match or are more specific than the given network/length. • **first-match**—Displays the first entry of the specified prefix list that matches the given network/length.

Command Default

If you do not specify a prefix list name, this command shows all of the prefix lists. If you do not include other keywords, the output shows the prefix list entries only.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Prefix lists are used in routing as matching criteria for route maps and policy lists.

Examples

The following is sample output from the **show ipv6 prefix-list** command.

```
ciscoasa(config)# show ipv6 prefix-list

ipv6 prefix-list test-ipv6-prefix: 1 entries
   seq 5 permit 2001:db8:0:cd30::/64
```

The following is an example of summarized output.

```
ciscoasa(config)# show ipv6 prefix-list summary

Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
```

The following is an example of detailed output.

```
ciscoasa(config)# show ipv6 prefix-list detail

Prefix-list with the last deletion/insertion: test-ipv6-prefix
ipv6 prefix-list test-ipv6-prefix:   count: 1, range entries: 0,
sequences: 5 - 5, refcount: 2
   seq 5 permit 2001:db8:0:cd30::/64 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
ipv6 prefix-list	Configures IPv6 prefix lists.

show ipv6 route management-only

To display the contents of the IPv6 routing table, use the **show ipv6 route** command in privileged EXEC mode. The management-only keyword displays routes in the IPv6 management routing table.

show ipv6 route management-only [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]

Syntax Description

managment-only	Displays routes in the IPv6 management routing table.
cluster	(Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number in a cluster.
failover	(Optional) Displays the IPv6 routing table sequence number, IPv6 reconvergence timer status, and IPv6 routing entries sequence number.
interface	(Optional) Displays IPv6 interface-specific routes.
ospf	(Optional) Displays OSPFv3 routes.
summary	(Optional) Displays IPv6 route summaries.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for the **failover, cluster, ospf, interface,** and **summary** keywords was added.
9.5(1)	Support for the management routing table feature was added.

Usage Guidelines

The **show ipv6 route** command provides output similar to the **show route** command, except that the information is IPv6-specific.

The following information appears in the IPv6 routing table:

- Codes—Indicates the protocol that derived the route. Values are as follows:
- C—Connected
- L—Local

- S—Static
- R—RIP derived
- B—BGP derived
- I1—ISIS L1—Integrated IS-IS Level 1 derived
- I2—ISIS L2—Integrated IS-IS Level 2 derived
- IA—ISIS interarea—Integrated IS-IS interarea derived
- fe80::/10—Indicates the IPv6 prefix of the remote network.
- [0/0]—The first number in the brackets is the administrative distance of the information source; the second number is the metric for the route.
- via ::—Specifies the address of the next router to the remote network.
- inside—Specifies the interface through which the next router to the specified network can be reached.

Note The **clustering** and **failover** keywords do not appear unless these features are configured on the ASA.

Examples

The following is sample output from the **show ipv6 route** command:

```
ciscoasa# show ipv6 route
IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

The following is sample output from the **show ipv6 route failover** command:

```
ciscoasa# show ipv6 route failover
IPv6 Routing Table - 6 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
           ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 0
IPv6 Reconvergence timer expired
```

```
O   2009::1/128 [110/10]
     via fe80::217:94ff:fe85:4401, inside seq 0
OE2  2011::/64 [110/20]
     via fe80::217:94ff:fe85:4401, inside seq 0
S   4001::1/128 [0/0]
     via 4001::2, inside seq 0
C   7001::1/128 [0/0]
     via ::, outside seq 0
L   fe80::/10 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
L   ff00::/8 [0/0]
     via ::, inside seq 0
     via ::, outside seq 0
```

The following is sample output from the **show ipv6 route cluster** command on the master unit:

```
ciscoasa/LB1/master(config)# show ipv6 route cluster
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 2
IPv6 Reconvergence timer expired
OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

The following is sample output from the **show ipv6 route cluster** command on the slave unit during a role change:

```
ciscoasa/LB2/slave(config)# cluster master
INFO: Wait for existing master to quit. Use "show cluster info"
to check status. Use "cluster remove unit <name>" to force
master unit out of the cluster if for some reason it refuses
to quit within reasonable time
ciscoasa/LB2/slave(config)#
ciscoasa/LB2/master(config)#
ciscoasa/LB2/master(config)# show ipv6 route cluster
IPv6 Routing Table - 5 entries
Codes: C - Connected, L - Local, S - Static
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
            ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
IPv6 Routing table seq num 3
IPv6 Reconvergence timer expires in 61 secs
OE2  2001::/58 [110/20]
     via fe80::21f:9eff:fe2a:78ba, inside seq 2
...
```

Related Commands

Command	Description
debug ipv6 route	Displays debugging messages for IPv6 routing table updates and route cache updates.
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 routers

To display IPv6 router advertisement information received from on-link routers, use the **show ipv6 routers** command in privileged EXEC mode.

show ipv6 routers [*if_name*]

Syntax Description

if_name	(Optional) The internal or external interface name, as designated by the **nameif** command, that you want to display information about.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

When an interface name is not specified, information on all IPv6 interfaces is displayed. Specifying an interface name displays information about the specified interface.

Examples

The following is sample output from the **show ipv6 routers** command when entered without an interface name:

```
ciscoasa# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

Related Commands

Command	Description
ipv6 route	Adds a static entry to the IPv6 routing table.

show ipv6 traffic

To display statistics about IPv6 traffic, use the **show ipv6 traffic** command in privileged EXEC mode.

show ipv6 traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **clear ipv6 traffic** command to clear the traffic counters.

Examples

The following is sample output from the **show ipv6 traffic** command:

```
ciscoasa# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent
ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
```

```
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert
UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output
TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

Related Commands

Command	Description
clear ipv6 traffic	Clears IPv6 traffic counters.

show is - show m

show isakmp ipsec-over-tcp stats

To display runtime statistics for IPsec over TCP, use the **show isakmp ipsec-over tcp stats** command in global configuration mode or privileged EXEC mode.

show isakmp ipsec-over-tcp stats

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
ASA virtual(1)	The **show isakmp ipsec-over-tcp stats** command was added.
7.2(1)	The **show isakmp ipsec-over-tcp stats** command was deprecated. The **show crypto isakmp ipsec-over-tcp stats** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The output from this command includes the following fields:

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets

- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures
- Checksum errors
- Internal errors

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
ciscoasa(config)# show isakmp ipsec-over-tcp stats
Global IPsec over TCP Statistics
--------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure crypto isakmp	Clears all the ISAKMP configuration.
clear configure crypto isakmp policy	Clears all ISAKMP policy configuration.
clear crypto isakmp sa	Clears the IKE runtime SA database.
crypto isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config crypto isakmp	Displays all the active ISAKMP configuration.

show isakmp sa

To display the IKE runtime SA database, use the **show isakmp sa** command in global configuration mode or privileged EXEC mode.

show isakmp sa [**detail**]

Syntax Description

detail	Displays detailed output about the SA database.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	The **show isakmp sa** command was added.
7.2(1)	This command was deprecated. The **show crypto isakmp sa** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The output from this command includes the following fields:

Detail not specified.

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

Detail specified.

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

Examples

The following example, entered in global configuration mode, displays detailed information about the SA database:

```
ciscoasa(config)# show isakmp sa detail
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
IKE Peer   Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isakmp stats

To display runtime statistics, use the **show isakmp stats** command in global configuration mode or privileged EXEC mode.

show isakmp stats

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
ASA virtual(1)	The **show isakmp stats** command was added.
7.2(1)	This command was deprecated. The **show crypto isakmp stats** command replaced it.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Each one of the counters maps to an associated cikePhase1GW counter. For details on each of these counters, refer to CISCO-IPSEC-FLOW-MONITOR-MIB.my .

- Active/Standby Tunnels—cikePhase1GWActiveTunnels
- Previous Tunnels—cikePhase1GWPreviousTunnels
- In Octets—cikePhase1GWInOctets
- In Packets—cikePhase1GWInPkts
- In Drop Packets—cikePhase1GWInDropPkts
- In Notifys—cikePhase1GWInNotifys
- In P2 Exchanges—cikePhase1GWInP2Exchgs
- In P2 Exchange Invalids—cikePhase1GWInP2ExchgInvalids

- In P2 Exchange Rejects—cikePhase1GWInP2ExchgRejects
- In P2 Sa Delete Requests—cikePhase1GWInP2SaDelRequests
- Out Octets—cikePhase1GWOutOctets
- Out Packets—cikePhase1GWOutPkts
- Out Drop Packets—cikePhase1GWOutDropPkts
- Out Notifys—cikePhase1GWOutNotifys
- Out P2 Exchanges—cikePhase1GWOutP2Exchgs
- Out P2 Exchange Invalids—cikePhase1GWOutP2ExchgInvalids
- Out P2 Exchange Rejects—cikePhase1GWOutP2ExchgRejects
- Out P2 Sa Delete Requests—cikePhase1GWOutP2SaDelRequests
- Initiator Tunnels—cikePhase1GWInitTunnels
- Initiator Fails—cikePhase1GWInitTunnelFails
- Responder Fails—cikePhase1GWRespTunnelFails
- System Capacity Fails—cikePhase1GWSysCapFails
- Auth Fails—cikePhase1GWAuthFails
- Decrypt Fails—cikePhase1GWDecryptFails
- Hash Valid Fails—cikePhase1GWHashValidFails
- No Sa Fails—cikePhase1GWNoSaFails

The output from this command includes the following fields:

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets

- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects
- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

Examples

The following example, issued in global configuration mode, displays ISAKMP statistics:

```
ciscoasa(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
isakmp enable	Enables ISAKMP negotiation on the interface on which the IPsec peer communicates with the ASA.
show running-config isakmp	Displays all the active ISAKMP configuration.

show isis database

To display the IS-IS link-state database, use the **show isis database** command in privileged EXEC mode.

show isis database [{ **detail** | **verbose** } [**ip** [**unicast**] | **ipv6** [**unicast**]] [**topology base**]] [**level-1** | **level-2**]

Syntax Description

level-1	(Optional) Displays the IS-IS link-state database for Level 1.
level-2	(Optional) Displays the IS-IS link-state database for Level 2.
ip	(Optional) Shows the IS-IS link-state database for the IPv4 address-family
ipv6	(Optional) Shows the IS-IS link-state database for the IPv6 address-family
detail	(Optional) Displays the contents of each link-state packet (LSP).
verbose	(Optional) Displays additional information about the Intermediate IS-IS database.
topology base	(Optional) Shows the MTR topology.
unicast	(Optional) Shows unicast address families.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

This command displays the IS-IS link-state database.

Examples

The following is sample output from the **show isis database** command:

```
ciscoasa# show isis database
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d300     0x3d0d            674                      0/0/0
```

```
routerA.00-00     0x1b541556     0xa349              928                    0/0/0
c3.00-00            0x9257c979     0x9952              759                    0/0/0
c2.00-00           *0xef11e977     0x3188              489                    0/0/0
c2.01-00           *0xa8333f03     0xd6ea              829                    0/0/0
IS-IS Level-2 Link State Database:
LSPID               LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00            0x63871f24      0xaba2              526                   0/0/0
routerA.00-00     0x0d540b55      0x81d7              472                   0/0/0
routerA.00-01     0xffffff01          0xe20b             677                    0/0/0
c3.00-00            0x002e5434      0xb20a            487                     0/0/0
c2.00-00           *0x74fd1227      0xbb0f            742                     0/0/0
c2.01-00           *0x7ee72c1a      0xb506            968                     0/0/0
```

Table 61: show isis database Fields

Field	Description
LSPID	The LSP identifier. The first six octets form the system ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is nonzero, the LSP describes links from the system. When it is zero, the LSP is a so-called nonpseudonode LSP. This mechanism is similar to a router link-state advertisement (LSA) in the Open Shortest Path First (OSPF) protocol. The LSP will describe the state of the originating router. For each LAN, the designated router for that LAN will create and flood a pseudonode LSP, describing all systems attached to that LAN. The last octet is the LSP number. If there is more data than can fit in a single LSP, the LSP will be divided into multiple LSP fragments. Each fragment will have a different LSP number. An asterisk (*) indicates that the LSP was originated by the system on which this command is issued.
LSP Seq Num	Sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from the link-state database (LSDB) of all routers. The value indicates how long the purged LSP will stay in the LSDB before being completely removed.
ATT	The Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 2 routers will use the Attach bit to find the closest Level 2 router. They will point a default route to the closest Level 2 router.
P	The P bit. Detects if the intermediate systems is area partition repair-capable. Cisco and other vendors do not support area partition repair.
OL	The Overload bit. Determines if the IS is congested. If the Overload bit is set, other routers will not use this system as a transit router when calculating routers. Only packets for destinations directly connected to the overloaded router will be sent to this router.

The following is sample output from the **show isis database detail** command. As the output shows, in addition to the information displayed with the **show isis database** command, the **show isis database detail** command displays the contents of each LSP.

```
ciscoasa# show isis database detail
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0xea19d301      0x3b0e              1189                    0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00      0x1b541556     0xa349              642                       0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IP 10.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Table 62: show isis database detail Fields

Field	Description
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).

The following is additional sample output from the **show isis database detail** command. This LSP is a Level 2 LSP. The area address 39.0001 is the address of the area in which the router resides.

```
ciscoasa# show isis database 12 detail
IS-IS Level-2 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00              0x63871f25      0xa9a3              1076                    0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   10.22.22.1
  Metric:         10 IS c2.01
routerA.00-00     0x0d540b56     0x7fd8              941                       0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   10.22.22.5
  Metric:         10 IS c2.01
  Metric:          0 IP-External 1.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.1.1.0 255.255.255.0
  Metric:          0 IP-External 2.2.2.0 255.255.255.0
  Metric:          0 IP-External 3.1.1.0 255.255.255.0
```

The following is sample output from the **show isis database verbose** command:

```
ciscoasa# show isis database verbose
IS-IS Level-1 Link State Database:
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
c1.00-00             *0xea19d301   0x3b0e        644              0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: c1
  IP Address:   22.22.22.1
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
routerA.00-00         0x1b541557   0xa14a        783              0/0/0
  Area Address: 49.0001
  NLPID:        0xcc
  Hostname: routerA
  IP Address:   22.22.22.5
  Metric:         10 IP 22.22.22.0 255.255.255.0
  Metric:         10 IS c2.01
```

Table 63: show isis database verbose Fields

Field	Description
LSPID	Link-state packet (LSP) identifier. The first six octets form the System ID of the router that originated the LSP. The next octet is the pseudonode ID. When this byte is zero, the LSP describes links from the system. When it is nonzero, the LSP is a pseudonode LSP. This is similar to a router LSA in Open Shortest Path First (OSPF); the LSP describes the state of the originating router. For each LAN, the designated router for that LAN creates and floods a pseudonode LSP that describes all systems attached to that LAN. The last octet is the LSP number. If all the data cannot fit into a single LSP, the LSP is divided into multiple LSP fragments. Each fragment has a different LSP number. An asterisk (*) indicates that the system issuing this command originated the LSP.
LSP Seq Num	LSP sequence number that allows other systems to determine if they received the latest information from the source.
LSP Checksum	Checksum of the entire LSP packet.
LSP Holdtime	Amount of time that the LSP remains valid (in seconds). An LSP hold time of zero indicates that this LSP was purged and is being removed from all routers' link-state databases (LSDBs). The value indicates how long the purged LSP will stay in the LSDB before it is completely removed.
ATT	Attach bit. This bit indicates that the router is also a Level 2 router, and it can reach other areas. Level 1 routers use the Attach bit to find the closest Level 2 router. They install a default route to the closest Level 2 router.
P	P bit. This bit detects if the IS can repair area partitions. Cisco and other vendors do not support area partition repair.
OL	Overload bit. This bit determines if the IS is congested. If the overload bit is set, other routers do not use this system as a transit router when they calculate routes. Only packets for destinations directly connected to the overloaded router are sent to this router.

Field	Description
Area Address	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
NLPID	Network Layer Protocol identifier.
Hostname	Hostname of the node.
Router ID	Traffic engineering router identifier for the node.
IP Address	IPv4 address for the interface.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system (ES), or a Connectionless Network Service [CLNS] prefix).
Affinity	Link attribute flags that are being flooded.
Physical BW	Link bandwidth capacity (in bits per second).
Reservable BW	Amount of reservable bandwidth on this link.
BW Unreserved	Amount of bandwidth that is available for reservation.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.

Command	Description
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.

Command	Description
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis hostname

To display the router-name-to-system-ID mapping table entries for an IS-IS router, use the **show isis hostname** command in privileged EXEC mode.

show isis hostname

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

In the IS-IS routing domain, the system ID is used to represent each router. The system ID is part of the network entity title (NET) that is configured for each IS-IS router. For example, a router with a configured NET of 49.0001.0023.0003.000a.00 has a system ID of 0023.0003.000a. Router-name-to-system-ID mapping is difficult for network administrators to remember during maintenance and troubleshooting on the routers. Entering the **show isis hostname** command displays the entries in the router-name-to-system-ID mapping table.

If the dynamic hostname feature has not been disabled by entering the **no hostname dynamic** command, the mapping will consist of a dynamic host mapping table.

Examples

The following example changes the hostname to ciscoASA and assigns the NET 49.0001.0050.0500.5005.00 to ciscoASA:

```
ciscoasa(config)# hostname ciscoASA
ciscoASA(config)# router isis
ciscoASA(config-router)# net 49.0001.0050.0500.5005.00
ciscoASA(config-router)# hostname dynamic
ciscoASA(config-router)#
```

Entering the **show isis hostname** command displays the dynamic host mapping table. The dynamic host mapping table displays the router-name-to-system-ID mapping table entries for ciscoASA, c2, c3 and for the local router named routerA. The table also shows that c3 is a Level-1 router, and its hostname is advertised by the Level-1 (L1) link-state protocol (LSP). C2 is a Level-2 router and its hostname is advertised by the L2 LSP. The * symbol that appears under Level for the ASA ciscoASA signifies that this is the router-name-to-system-ID mapping information for the ASA.

```
ciscoASA# show isis hostname
Level  System ID       Dynamic Hostname  (c1)
     * 0050.0500.5005   ciscoASA
    1  0050.0500.5007   c3
    2  0050.0500.5006   routerA
    2  0050.0500.5008   c2
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).

Command	Description
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.

Command	Description
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis lsp-log

To display the Level 1 and Level 2 IS-IS link-state packet (LSP) log of the interfaces that triggered the new LSP, use the **show isis lsp-log** command in privileged EXEC mode.

show isis lsp-log

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

Displays the Level 1 and Level 2 IS-IS link-state packet (LSP) log of the interfaces that triggered the new LSP.

Examples

The following is sample output from the **show isis lsp-log** command:

```
ciscoasa# show isis lsp-log
    Level 1 LSP log
  When       Count       Interface         Triggers
  04:16:47     1         subint             CONFIG NEWADJ DIS
  03:52:42     2         subint             NEWADJ DIS
  03:52:12     1         subint             ATTACHFLAG
  03:31:41     1         subint             IPUP
  03:30:08     2         subint             CONFIG
  03:29:38     1         subint             DELADJ
  03:09:07     1         subint             DIS ES
  02:34:37     2         subint             NEWADJ
  02:34:07     1         subint             NEWADJ DIS
    Level 2 LSP log
  When       Count       Interface         Triggers
  03:09:27     1         subint             CONFIG NEWADJ
  03:09:22     1         subint             NEWADJ
  02:34:57     2         subint             DIS
  02:34:50     1                                IPUP
  02:34:27     1         subint             CONFIG DELADJ
  02:13:57     1         subint             DELADJ
  02:13:52     1         subint             NEWADJ
```

```
 01:35:58     2         subint             IPIA
 01:35:51     1                               AREASET IPIA
```

Table 64: show isis lsp-log Fields

Field	Description
When	Time elapsed since the LSP was generated.
Count	Number of events that took place at this time.
Interface	Interface that caused the LSP regeneration.
Triggers	Event that triggered the LSP to be flooded. Possible triggers for an LSP are as follows: • AREASET—Active area set changed. • ATTACHFLAG—Attach bit changed state. • CLEAR—Some form of manual clear command was issued. • CONFIG—Any configuration change. • DELADJ—Adjacency went down. • DIS—DIS changed or pseudonode changed. • ES—End System adjacency changed. • HIPPITY—LSPDB overload bit changed state. • IF_DOWN—Needs a new LSP. • IP_DEF_ORIG—Default information originate changed. • IPDOWN—Directly connected IP prefix down. • IP_EXTERNAL—Redistributed IP route appeared or gone. • IPIA—Interarea IP route appeared or gone. • IPUP—Directly connected IP prefix up. • NEWADJ—New adjacency came up. • REDIST—Redistributed level-2 CLNS route changed. • RRR_INFO—RRR bandwidth resource information.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis neighbors

To display information about IS-IS neighbors, use the **show isis neighbors** command in privileged EXEC mode.

show isis neighbors [**detail**]

Syntax Description

detail	(Optional) Displays more detailed information for IS-IS neighbors.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

The **show isis neighbors** command is used to display brief information about connected IS-IS routers. Enter the **detail** keyword to display more detailed information.

Examples

The show **isis neighbors command** is entered to display information about the IS-IS neighbor routerA:

```
ciscoasa# show isis neighbors
System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint        22.22.22.5        UP    21             c2.01
routerA          L2    subint        22.22.22.5        UP    22             c2.01
c2                   L1    subint        22.22.22.3        UP     9             c2.01
c2                   L2    subint        22.22.22.3        UP     9             c2.01
```

The **show isis neighbors detail** command is entered to display more detailed information about the IS-IS neighbor routerA:

```
ciscoasa# show isis neighbors detail
System Id      Type Interface   IP Address      State Holdtime Circuit Id
routerA          L1    subint        22.22.22.5        UP    23             c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
routerA          L2    subint        22.22.22.5        UP    22             c2.01
  Area Address(es): 49.0001
  SNPA:       0025.8407.f2b0
  State Changed: 00:03:03
  LAN Priority: 64
  Format: Phase V
  Remote TID: 0
  Local TID:  0
  Interface name: subint
```

Table 65: show isis neighbors Fields

Field	Description
System Id	Six-byte value that identifies a system in an area.
Type	Level type. Indicates whether the IS-IS neighbor is a Level 1, Level-1-2, or Level 2 router.
Interface	Interface from which the system was learned.
IP Address	IP address of the neighbor router.
State	Indicates whether the state of the IS-IS neighbor is up or down.
Holdtime	Link-state packet (LSP) holdtime. Amount of time that the LSP remains valid (in seconds).
Circuit Id	Port location for the IS-IS neighbor router that indicates how it is connected to the local router.
Area Address(es)	Reachable area addresses from the router. For Level 1 LSPs, these are the area addresses configured manually on the originating router. For Level 2 LSPs, these are all the area addresses for the area to which this router belongs.
SNPA	Subnetwork point of attachment. This is the data-link address.
State Changed	State change.
LAN Priority	Priority of the LAN.
Remote TID	Neighbor router topology ID(s).
Local TID	Local router topology ID(s).

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.

Command	Description
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.

Command	Description
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.

Command	Description
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis rib

To display paths for a specific route or for all routes under a major network that are stored in the IP local Routing Information Base (RIB), use the **show isis rib** command in privileged EXEC mode.

show isis [***|** **ip** [**unicast**] **| ipv6** [**unicast**]] **rib** [**redistribution** [**level-1 | level-2**]] [*network_ip* [*mask*]]

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
level-1	(Optional) Shows the Level 1 redistribution RIB.
level-2	(Optional) Shows the Level 2 redistribution RIB
network_ip [*mask*]	(Optional) Shows RIB information for a network.
redistribution	(Optional) Shows IS-IS IP redistribution RIB information
unicast	(Optional) Shows the unicast address family.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

To verify that an IP prefix update that exists in the IP global RIB also has been updated in the IS-IS local RIB, enter the **show isis rib** command.

Examples

The following is sample output from the **show isis rib** command to show all routes that are stored within the IS-IS local RIB:

```
ciscoasa# show isis rib
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = = =
10.10.0.0 255.255.0.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

The following is sample output from the **show isis rib** command to show all routes under the major network 10.0.0.0 with the IP address 10.3.2.0 that are stored within the IS-IS local RIB:

```
ciscoasa# show isis rib 10.3.2.0
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =
Routes under majornet 10.0.0.0 255.0.0.0:
10.1.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[12/524]
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

The following is sample output from the **show isis rib** command to show all routes under the network with the IP address mask 10.3.2.0 255.255.255.0 that are stored within the IS-IS local RIB:

```
ciscoasa# show isis rib 10.3.2.0 255.255.255.0
IPv4 local RIB for IS-IS process
IPV4 unicast topology base (TID 0, TOPOID 0x2) = = = = = = = = = = = = =
10.3.2.0 255.255.255.0
  [115/L2/10] via 10.22.22.5(subint), from 10.22.22.5, tag 0, LSP[13/149]
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.

Command	Description
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.

Command	Description
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis spf-log

To display how often and why the router has run a full shortest path first (SPF) calculation, use the **show isis spf-log** command in privileged EXEC mode.

show isis [***| ip** [**unicast**] **| ipv6** [**unicast**]] **spf-log**

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
unicast	(Optional) Shows the unicast address family.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command Modes

The following table shows the modes in which you can enter the command:

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

This command displays how often and why the router has run a full shortest path first (SPF) calculation.

Examples

The following is sample output from the **show isis ipv6 spf-log** command:

```
ciscoasa# show isis ipv6 spf-log
      TID 0 level 1 SPF log
  When   Duration  Nodes  Count     First trigger LSP   Triggers
00:15:46    3124     40      1          milles.00-00  TLVCODE
00:15:24    3216     41      5          milles.00-00  TLVCODE NEWLSP
00:15:19    3096     41      1          deurze.00-00  TLVCODE
00:14:54    3004     41      2          milles.00-00  ATTACHFLAG LSPHEADER
00:14:49    3384     41      1          milles.00-01  TLVCODE
00:14:23    2932     41      3          milles.00-00  TLVCODE
00:05:18    3140     41      1                        PERIODIC
00:03:54    3144     41      1          milles.01-00  TLVCODE
00:03:49    2908     41      1          milles.01-00  TLVCODE
00:03:28    3148     41      3           bakel.00-00  TLVCODE TLVCONTENT
```

```
00:03:15    3054     41      1          milles.00-00  TLVCODE
00:02:53    2958     41      1          mortel.00-00  TLVCODE
00:02:48    3632     41      2          milles.00-00  NEWADJ TLVCODE
00:02:23    2988     41      1          milles.00-01  TLVCODE
00:02:18    3016     41      1          gemert.00-00  TLVCODE
00:02:14    2932     41      1           bakel.00-00  TLVCONTENT
00:02:09    2988     41      2           bakel.00-00  TLVCONTENT
00:01:54    3228     41      1          milles.00-00  TLVCODE
00:01:38    3120     41      3            rips.03-00  TLVCONTENT
```

Table 66: show isis spf-log Fields

Field	Description
When	How long ago (in hours: minutes: seconds) a full SPF calculation occurred. The last 20 occurrences are logged.
Duration	Number of milliseconds required to complete this SPF run. Elapsed time is wall clock time, not CPU time.
Nodes	Number of routers and pseudonodes (LANs) that make up the topology calculated in this SPF run.
Count	Number of events that triggered this SPF run. When there is a topology change, often multiple link-state packets (LSPs) are received in a short time. A router waits 5 seconds before running a full SPF run, so it can include all new information. This count denotes the number of events (such as receiving new LSPs) that occurred while the router was waiting its 5 seconds before running full SPF.
First trigger LSP	Whenever a full SPF calculation is triggered by the arrival of a new LSP, the router stores the LSP ID. The LSP ID can provide a clue as to the source of routing instability in an area. If multiple LSPs are causing an SPF run, only the LSP ID of the last received LSP is remembered.
Triggers	A list of all reasons that triggered a full SPF calculation. See the next table for triggers.

Table 67: spf-log Triggers

Trigger	Description
ATTACHFLAG	This router is now attached to the Level 2 backbone or it has just lost contact to the Level 2 backbone.
ADMINDIST	Another administrative distance was configured for the IS-IS process on this router.
AREASET	Set of learned area addresses in this area changed.
BACKUPOVFL	An IP prefix disappeared. The router knows there is another way to reach that prefix but has not stored that backup route. The only way to find the alternative route is through a full SPF run.
DBCHANGED	A clear isis * command was issued on this router.

Trigger	Description
IPBACKUP	An IP route disappeared, which was not learned via IS-IS, but via another protocol with better administrative distance. IS-IS will run a full SPF to install an IS-IS route for the disappeared IP prefix.
IPQUERY	A clear ip route command was issued on this router.
LSPEXPIRED	Some LSP in the link-state database (LSDB) has expired.
LSPHEADER	ATT/P/OL bits or is-type in an LSP header changed.
NEWADJ	This router has created a new adjacency to another router.
NEWAREA	A new area (via network entity title [NET]) was configured on this router.
NEWLEVEL	A new level (via is-type) was configured on this router.
NEWLSP	A new router or pseudonode appeared in the topology.
NEWMETRIC	A new metric was configured on an interface of this router.
NEWSYSID	A new system ID (via NET) was configured on this router.
PERIODIC	Typically, every 15 minutes a router runs a periodic full SPF calculation.
RTCLEARED	A clear clns route command was issued on this router.
TLVCODE	TLV code mismatch, indicating that different TLVs are included in the newest version of an LSP.
TLVCONTENT	TLV contents changed. This normally indicates that an adjacency somewhere in the area has come up or gone down. The "First trigger LSP" column indicates where the instability may have occurred.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.

Command	Description
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.

Command	Description
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.

Command	Description
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show isis topology

To display a list of all connected routers in all areas, use the **show isis topology** command in privileged EXEC mode.

show isis [***| ip** [**unicast**] **| ipv6** [**unicast**]] **topology** [**level-1 | level-2**]

Syntax Description

*****	(Optional) Shows all IS-IS address families.
ip	(Optional) Shows the IPv4 address family.
ipv6	(Optional) Shows the IPv6 address family.
level-1	(Optional) Shows paths to all level-1 routers in the area.
level-2	(Optional) Shows paths to all level-2 routers in the domain.
unicast	(Optional) Shows the unicast address family.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

Use the **show isis topology** command to verify the presence and connectivity between all routers in all areas.

Examples

The following example shows output from the **show isis topology** command.

```
ciscoasa# show isis topology

IS-IS TID 0 paths to level-1 routers
System Id            Metric     Next-Hop             Interface   SNPA
cisco1                 --
routerA               10           routerA                 subint       0025.8407.f2b0
c3                        10
c2                        10           c2                              subint
c08c.60e6.986f
```

```
IS-IS TID 0 paths to level-2 routers
System Id            Metric     Next-Hop            Interface   SNPA
cisco1                 --
routerA               10            routerA                subint       0025.8407.f2b0
c3                       10
c2                      10           c2                       subint       c08c.60e6.986f
```

Table 68: show isis topology Fields

Field	Description
System Id	Six-byte value that identifies a system in an area.
Metric	IS-IS metric for the cost of the adjacency between the originating router and the advertised neighbor, or the metric of the cost to get from the advertising router to the advertised destination (which can be an IP address, an end system [ES], or a CLNS prefix).
Next-Hop	The address of the next hop router.
Interface	Interface from which the system was learned.
SNPA	Subnetwork point of attachment. This is the data-link address.

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.

Command	Description
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.

Command	Description
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

show kernel

To display information that the Linux brctl utility provides that you can use for debugging, use the **show kernel** command in privileged EXEC mode.

show kernel [**process** | **bridge** | **cgroup-controller** | **ifconfig** | **module**]

Syntax Description

bridge	Displays tap bridges.
cgroup-controller	Displays the cgroup-controller statistics.
ifconfig	Displays the tap and bridge interface statistics.
module	Displays the modules that are installed and running.
process	Displays the current status of the active kernel processes running on the ASA.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.
8.4(1)	The **cgroup-controller** keyword was added.
8.6(1)	The **ifconfig**, **module**, and **bridge** keywords were added.

Usage Guidelines

This command displays statistics for the various processes running on the kernel.

Examples

The following example displays output from the **show kernel process** command:

```
ciscoasa# show kernel process
PID PPID PRI NI      VSIZE      RSS      WCHAN STAT  RUNTIME COMMAND
  1    0  16  0     991232      268 3725684979    S       78 init
  2    1  34 19          0        0 3725694381    S        0 ksoftirqd/0
  3    1  10 -5          0        0 3725736671    S        0 events/0
  4    1  20 -5          0        0 3725736671    S        0 khelper
  5    1  20 -5          0        0 3725736671    S        0 kthread
  7    5  10 -5          0        0 3725736671    S        0 kblockd/0
  8    5  20 -5          0        0 3726794334    S        0 kseriod
 66    5  20  0          0        0 3725811768    S        0 pdflush
 67    5  15  0          0        0 3725811768    S        0 pdflush
 68    1  15  0          0        0 3725824451    S        2 kswapd0
 69    5  20 -5          0        0 3725736671    S        0 aio/0
171    1  16  0     991232       80 3725684979    S        0 init
172  171  19  0     983040      268 3725684979    S        0 rcS
201  172  21  0    1351680      344 3725712932    S        0 lina_monitor
202  201  16  0 1017602048   899932 3725716348    S      212 lina
203  202  16  0 1017602048   899932          0    S        0 lina
204  203  15  0 1017602048   899932          0    S        0 lina
205  203  15  0 1017602048   899932 3725712932    S        6 lina
206  203  25  0 1017602048   899932          0    R 13069390 lina
ciscoasa#
```

Table 9-9 shows each field description.

Table 69: show kernel process Fields

Field	Description
PID	The process ID.
PPID	The parent process ID.
PRI	The priority of the process.
NI	The nice value, which is used in priority computation. The values range from 19 (nicest) to -19 (not nice to others),
VSIZE	The virtual memory size in bytes.
RSS	The resident set size of the process, in kilobytes.
WCHAN	The channel in which the process is waiting.
STAT	The state of the process: • R—Running • S—Sleeping in an interruptible wait • D—Waiting in an uninterruptible disk sleep • Z—zombie • T—Traced or stopped (on a signal) • P—Paging
RUNTIME	The number of jiffies that the process has been scheduled in user mode and kernel mode. The runtime is the sum of utime and stime.
COMMAND	The process name.

Examples

The following example displays output from the **show kernel module** command:

```
ciscoasa# show kernel module
Module                  Size  Used by    Tainted: P
cpp_base              861808  2
kvm_intel              44104  8
kvm                   174304  1 kvm_intel
msrif                   4180  0
tscsync                 3852  0
```

The following example displays output for the **show kernel ifconfig** commands:

ciscoasa# **show kernel ifconfig**

```
br0       Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:43 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1708 (1.6 KiB)  TX bytes:0 (0.0 B)
br1       Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.255.255.255
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
tap0      Link encap:Ethernet  HWaddr 6A:0C:48:32:FE:F4
          inet addr:127.0.2.2  Bcast:127.255.255.255  Mask:255.0.0.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:148 errors:0 dropped:0 overruns:0 frame:0
          TX packets:186 errors:0 dropped:13 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:10320 (10.0 KiB)  TX bytes:12452 (12.1 KiB)
tap1      Link encap:Ethernet  HWaddr 8E:E7:61:CF:E9:BD
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:187 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:19368 (18.9 KiB)  TX bytes:14638 (14.2 KiB)
tap2      Link encap:Ethernet  HWaddr 6A:03:EC:BA:89:26
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
tap3      Link encap:Ethernet  HWaddr 42:9E:B8:6C:1F:23
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:187 errors:0 dropped:0 overruns:0 frame:0
          TX packets:256 errors:0 dropped:3 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:14638 (14.2 KiB)  TX bytes:19202 (18.7 KiB)
tap4      Link encap:Ethernet  HWaddr 6A:5C:60:BC:9C:ED
          UP BROADCAST RUNNING PROMISC MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Related Commands

Command	Description
show module	Shows information about the installed modules in the ASA.

show kernel bridge

To display the Linux bridges, their member ports, and MAC addresses that have been learned at each port that you can use for debugging, use the **show kernel bridge** command in privileged EXEC mode.

show kernel bridge [**mac-address** *bridge name*]

Syntax Description

bridge name	Displays the bridge name.
mac-address	Displays the MAC address associated with each port.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.6(1)	This command was added.

Usage Guidelines

This command shows the Linux bridges, their member ports, and the MAC addresses that have been learned at each port (including remote MAC addresses) that you can use for debugging.

Examples

The following example displays output from the **show kernel bridge** command:

```
ciscoasa# show kernel bridge
bridge name    bridge id        STP enabled interfaces
br0        8000.0e3cd8a8909f    no        tap1
                            tap3
br1       8000.26d29f51a490     no        tap2
                            tap4
                            tap5hostname#
```

The following example displays output from the **show kernel bridge mac-address** command:

```
ciscoasa# show kernel bridge mac-address br1
port no    mac addr       is local?   ageing timer
 1    00:21:d8:cb:dc:f7    no          12.93
 3    00:22:bd:d8:7d:da    no          12.93
 2    26:d2:9f:51:a4:90    yes          0.00
 1    4e:a4:e0:73:1f:ab    yes          0.00
 3    52:04:38:3d:79:c0    yes          0.00
```

Related Commands

Command	Description
show kernel	Shows information about the installed modules in the ASA.

show lacp

To display EtherChannel LACP information such as traffic statistics, system identifier, and neighbor details, enter this command in privileged EXEC mode.

show lacp { [*channel_group_number*] { **counters | internal | neighbor** } **sys-id** }

Syntax Description

channel_group_number	(Optional) Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
counters	Shows counters for the number of LACPDUs and markers sent and received.
internal	Shows internal information.
neighbor	Shows neighbor information.
sys-id	Shows the LACP system ID.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Examples

The following is sample output from the **show lacp sys-id** command:

```
ciscoasa# show lacp sys-id
32768,001c.c4e5.cfee
```

The following is sample output from the **show lacp counters** command:

```
ciscoasa# show lacp counters
             LACPDUs         Marker      Marker Response    LACPDUs
Port       Sent   Recv     Sent   Recv     Sent    Recv      Pkts Err
----------------------------------------------------------------------
Channel group: 1
Gi3/1      736    728      0      0         0      0         0
```

```
Gi3/2       739    730      0      0        0      0         0
Gi3/3       739    732      0      0        0      0         0
```

The following is sample output from the **show lacp internal** command:

```
ciscoasa# show lacp internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 1
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-----------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d
Gi3/3     SA      bndl       32768         0x1       0x1     0x304       0x3d
```

The following is sample output from the **show lacp neighbor** command:

```
ciscoasa# show lacp neighbor
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode
Channel group 1 neighbors
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

show lacp cluster

To show the cLACP system MAC and ID, use the **show lacp cluster** command in privileged EXEC mode.

show lacp cluster { **system-mac** | **system-id** }

Syntax Description

system-mac	Shows the system ID and whether it was auto-generated or entered manually.
system-id	Shows the system ID and priority.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Set the cLACP system ID and priority using the **clacp system-mac** command.

Examples

The following is sample output from the **show lacp cluster system-mac** command:

```
ciscoasa(cfg-cluster)# show lacp cluster system-mac
lacp cluster system MAC is automatically generated: a300.010a.010a.
```

The following is sample output from the **show lacp cluster system-id** command:

```
ciscoasa(cfg-cluster)# show lacp cluster system-id
5    ,a300.010a.010a
```

Related Commands

Command	Description
clacp system-mac	Sets the cLACP system ID and priority.

show license

To show smart licensing status, use the **show license** command in privileged EXEC mode.

Note This feature is supported on the ASA virtual only.

show license [**all** | **entitlement** | **cert** | **pool** | **registration** | **features**]

Syntax Description

all	Displays the state of Smart Licensing, Smart Agent version, UDI information, Smart Agent state, global compliance status, the entitlements status, licensing certificate information and schedule Smart Agent tasks.
entitlement	Displays detailed information about each entitlement in use, its handle (i.e. integer id), its count, tag, enforcement mode (e.g. in compliance, out of compliance, etc.), version and time at which the entitlement was requested.
cert	Displays the ID certificate content, date issued, and the date it expires.
pool	Displays the entitlement pool to which this device is assigned.
registration	Displays the current Smart License registration status.
features	Displays the current license.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

The **show activation-key** command provides the same output as the show license features command.

Examples

The following example shows an ASA virtual with only a base license (no current license entitlement):

```
Serial Number:  9AAHGX8514R
ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured
Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

show lisp eid

To view the ASA EID table, use the **show lisp eid** command in privileged EXEC mode.

show lisp eid [**site-id** *id*]

Syntax Description

site-id *id*	View only EIDs for a particular site.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

The ASA maintains an EID table that correlates the EID and the site ID. View the table with the **show lisp eid** command.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.

3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.
4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following is sample output from the **show lisp eid** command:

```
ciscoasa# show lisp eid
LISP EID       Site ID
10.44.33.105       2
10.44.33.201       2
192.168.11.1       4
192.168.11.2       4
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the pre-shared key to validate LISP messages.

show local-host

To display the network states of local hosts, use the **show local-host** command in privileged EXEC mode.

show local-host [*hostname* | *ip_address*] [**detail**] [**brief**] [**all**] [**connection** { **sctp** | **tcp** | **udp** | **embryonic** } *start* [*-end*]] [**zone** [*zone_name*]]

Syntax Description

all	(Deprecated) Includes local hosts connecting to the ASA and from the ASA.
brief	(Optional) Displays brief information on local hosts.
connection { **sctp** | **tcp** | **udp** | **embryonic** } *start* [*-end*]	(Deprecated) Applies filters based on the number and type of connections: embryonic, TCP, UDP, or SCTP. The *start* number indicates the minimum number of connections of that type. Include an - *end* number to specify a range, such as 10-100. These filters can be used individually or jointly.
detail	(Optional) Displays the detailed network states of local host information, including more information about active xlates and network connections.
hostname | *ip_address*	(Optional) Specifies the local host name or IPv4/IPv6 address.
zone [*zone_name*]	(Optional) Specifies local hosts per zone.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	For models with host limits, this command now shows which interface is considered to be the outside interface.
7.2(4)	Two new options, **connection** and **brief** , were added to the show local-host command so that the output is filtered by the number of connections for the inside hosts.
9.1(2)	The Smart Call Home information sent to Cisco for telemetry-based alerts from the **show local-host** command has been changed to the **show local-host | include interface** command. This provides interface address information.

Release	Modification
9.3(2)	The **zone** keyword was added.
9.5(2)	The display was modified to indicate backup port blocks with an asterisk (*).
9.5(2)	SCTP connections were added to the output. The **connection sctp** keyword was added.
9.14(1)	The connection filter keywords embryonic, TCP, UDP, or SCTP, were deprecated.
9.16(1)	Multicast data connection entries were added to the output.

Usage Guidelines

The **show local-host** command lets you display the network states of local hosts. A local-host is created for any host that forwards traffic to, or through, the ASA.

For systems running 9.16 and later, consider using the **show conn address** command instead of this one.

This command lets you show the translation and connection slots for the local hosts. Translation information includes any PAT port blocks allocated to the host.

For models with host limits, in routed mode, hosts on the inside (Work and Home zones) count towards the limit only when they communicate with the outside (Internet zone). Internet hosts are not counted towards the limit. Hosts that initiate traffic between Work and Home are also not counted towards the limit. The interface associated with the default route is considered to be the Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit.

Deprecated Options

This command also displays the connection limit values. If a connection limit is not set, the value displays as 0 and the limit is not applied.

In the event of a SYN attack (with TCP intercept configured), the **show local-host** command output includes the number of intercepted connections in the usage count. This field typically displays only full open connections.

In the **show local-host** command output, the **TCP embryonic count to host counter** is used when a maximum embryonic limit (TCP intercept watermark) is configured for a host using a static connection. This counter shows the total embryonic connections to the host from other hosts. If this total exceeds the maximum configured limit, TCP intercept is applied to new connections to the host.

Examples

The following is sample output from the **show local-host** command:

```
ciscoasa# show local-host
Interface mgmt: 2 active, 2 maximum active
local host: <10.24.250.191>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited
local host: <10.44.64.65>,
    SCTP flow count/limit = 0/unlimited
    TCP flow count/limit = 1/unlimited
    TCP embryonic count to host = 1
    TCP intercept watermark = unlimited
    UDP flow count/limit = 5/unlimited
```

```
Interface inside: 0 active, 0 maximum active,
Interface outside: 0 active, 0 maximum active
Interface any: 0 active, 0 maximum active, 0 denied
```

The following is sample output from the **show local-host** command on an ASA with host limits:

```
ciscoasa# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all other
interfaces.
Current host count: 3, towards licensed host limit of: 50
Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

The following is sample output from the **show local-host** command on an ASA with host limits. But without a default route, the host limits apply to all interfaces. The default route interface might not be detected if the default route or the interface that the route uses is down.

```
ciscoasa# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.
Current host count: 3, towards licensed host limit of: 50
Interface c1in: 1 active, 1 maximum active
Interface c1out: 0 active, 0 maximum active
```

The following is sample output from the **show local-host** command on an ASA with unlimited hosts:

```
ciscoasa# show local-host
Licensed host limit: Unlimited
Interface c1in: 1 active, 1 maximum active
Interface c1out: 0 active, 0 maximum active
```

The following example shows information about a specific host, followed by detailed information for that host.

```
ciscoasa# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)
Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active
ciscoasa# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active
Interface inside: 1 active, 1 maximum active
local host: <10.1.1.91>,
SCTP flow count/limit = 0/unlimited
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri
Conn:
```

```
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1 active,
1 maximum active
```

Related Commands

Command	Description
clear local-host	(Deprecated) Releases network connections from local hosts displayed by the **show local-host** command.
nat	Associates a network with a pool of global IP addresses.

show logging

To show the logs in the buffer or other logging settings, use the **show logging** command in privileged EXEC mode.

show logging [**message** [*syslog_id* | **all**] | **asdm** | **queue** | **setting** | **flow-export-syslogs**]
message

Syntax Description

all	(Optional) Displays all syslog message IDs, along with whether they are enabled or disabled.
asdm	(Optional) Displays ASDM logging buffer content.
flow-export-syslogs	(Optional) Displays the messages that are sent to Netflow, and whether they are enabled or disabled.
message	(Optional) Displays messages that are at a non-default level. See the **logging message** command to set the message level.
queue	(Optional) Displays the syslog message queue.
setting	(Optional) Displays the logging setting, without displaying the logging buffer.
syslog_id	(Optional) Specifies a message number to display.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	Indicates whether a syslog server is configured to use an SSL/TLS connection.
8.1(1)	The **flow-export-syslogs** keyword was added.
8.4(1)	For the **show logging** command, the output includes an entry for the current state of the audit block.
9.7(1)	The output from this command includes syslog servers configured with IPv6 addresses.

Usage Guidelines

If the logging buffered command is in use, the show logging command without any keywords shows the current message buffer and the current settings.

The show logging queue command allows you to display the following:

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them
- Separate queues for traps and other syslog messages

Note The `UDP Tx` in the output displays the number of syslog messages sent from the data engine.

Note Zero is an acceptable number for the configured queue size and represents the maximum queue size allowed. The output for the **show logging queue** command will display the actual queue size if the configured queue size is zero.

Examples

The following is sample output from the **show logging** command:

```
Timestamp logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 279951603 messages logged
    Trap logging: level debugging, facility 20, 1288748922 messages logged
        Logging to MGMT x.x.x.x errors: 2  dropped: 32
        Logging to MGMT x.x.x.x
        Logging to MGMT x.x.x.x
        Logging to MGMT x.x.x.x errors: 1  dropped: 2
    Permit-hostdown logging: state

    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

Note Valid values of *state* are enabled, disabled, disabled-blocking, and disabled-not blocking.

ASA stores maximum amount of logs per type per minute and drops the rest. You can use the following command to know the configured limit:

```
show running-config all logging | in rate-limit
```

You can modify the limit using `logging rate-limit`.

The following is sample output from the **show logging** command with a secure syslog server configured:

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure
ciscoasa(config)# show logging
Syslog logging: disabled
 Facility:
 Timestamp logging: disabled
 Deny Conn when Queue Full: disabled
 Console logging: level debugging, 135 messages logged
 Monitor logging: disabled
 Buffer logging: disabled
 Trap logging: list show _syslog, facility, 20, 21 messages logged
  Logging to inside 10.0.0.1 tcp/1500 SECURE
 History logging: disabled
 Device ID: disabled
 Mail logging: disabled
 ASDM logging disabled
```

The following is sample output from the **show logging queue** command:

```
ciscoasa(config)# show logging
            queue
Logging Queue length limit: 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msgs on queue, 0 msgs most on queue
```

The following is sample output from the **show logging message all** command:

```
ciscoasa(config)# show logging message all
syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

The following example shows the messages that are sent to Netflow, and whether they are enabled or disabled.

```
ciscoasa# show logging flow-export-syslogs

Syslog ID       Type                           Status
302013          Flow Created                   Enabled
302015          Flow Created                   Enabled
302017          Flow Created                   Enabled
302020          Flow Created                   Enabled
302014          Flow Deleted                   Enabled
302016          Flow Deleted                   Enabled
302018          Flow Deleted                   Enabled
302021          Flow Deleted                   Enabled
106015          Flow Denied                    Enabled
106023          Flow Denied                    Enabled
313001          Flow Denied                    Enabled
313008          Flow Denied                    Enabled
```

```
710003          Flow Denied                     Enabled
106100          Flow Created/Denied             Enabled
```

Related Commands

Command	Description
logging asdm	Enables logging to ASDM
logging buffered	Enables logging to the buffer.
logging flow-export-syslogs	Enables or disables syslog messages that are associated with NetFlow data.
logging host	Defines a syslog server.
logging message	Sets the message level or disables messages.
logging queue	Configures the logging queue.

show mac-address-table

To show the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

show mac-address-table [*interface_name* **| count | static | vtep-mapping**]

Syntax Description

count	(Optional) Lists the total number of dynamic and static entries.
interface_name	(Optional) Identifies the interface name for which you want to view MAC address table entries.
static	(Optional) Lists only static entries.
vtep-mapping	(Optional) Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.

Command Default

If you do not specify an interface, all interface MAC address entries are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.4(1)	The **vtep-mapping** keyword was added.
9.7(1)	Support for routed mode was added.

Examples

The following is sample output from the **show mac-address-table** command:

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
-----------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

The following is sample output from the **show mac-address-table** command for the inside interface:

```
ciscoasa# show mac-address-table
```

```
 inside
interface        mac address       type         Time Left
-----------------------------------------------------------------------
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

The following is sample output from the **show mac-address-table count** command:

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

See the following output for the **show mac-address-table vtep-mapping** command:

```
ciscoasa# show mac-address-table vtep-mapping
interface                    mac  address       type     Age(min)   bridge-group    VTEP
------------------------------------------------------------------------------------------
vni-outside                 00ff.9200.0000      dynamic      5          1        10.9.1.3
vni-inside                  0041.9f00.0000      dynamic      5          1      10.9.1.3
```

Related Commands

Command	Description
firewall transparent	Sets the firewall mode to transparent.
mac-address-table aging-time	Sets the timeout for dynamic MAC address entries.
mac-address-table static	Adds a static MAC address entry to the MAC address table.
mac-learn	Disables MAC address learning.

show mac-learn

To show whether MAC learning is enabled or disabled for each interface, use the **show mac-learn** command in privileged EXEC mode.

show mac-learn

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.7(1)	Support for routed mode was added.

Usage Guidelines

By default, each interface automatically learns the MAC addresses of entering traffic, and the system adds corresponding entries to the MAC address table. You can disable MAC learning per interface.

Examples

The following is sample output from the **show mac-learn** command.

```
ciscoasa# show mac-learn

no mac-learn flood
interface                          mac learn
-------------------------------------------
 outside                             enabled
 inside1_2                           enabled
 inside1_3                           enabled
 inside1_4                           enabled
 inside1_5                           enabled
 inside1_6                           enabled
 inside1_7                           enabled
 inside1_8                           enabled
 diagnostic                          enabled
 inside                              enabled
```

Related Commands

Command	Description
mac-learn	Disables MAC address learning.

show management-access

To display the name of the internal interface configured for management access, use the show management-access command in privileged EXEC mode.

show management-access

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **management-access** command lets you define an internal management interface using the IP address of the firewall interface specified in *mgmt_if*. (The interface names are defined by the **nameif** command and displayed in quotes, “ ”, in the output of the **show interface** command.)

Examples

The following example shows how to configure a firewall interface named “inside” as the management access interface and display the result:

```
ciscoasa(config)# management-access inside
ciscoasa(config)# show management-access
management-access inside
```

Related Commands

Command	Description
clear configure management-access	Removes the configuration of an internal interface for management access of the ASA.
management-access	Configures an internal interface for management access.

show-map-domain

To show the Mapping Address and Port (MAP) domain, use the **show map-domain** command in privileged EXEC mode.

show map-domain

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The **show map-domain** command displays the MAP configuration (similar to the **show running-config map-domain**), but also indicates whether a domain configuration is valid.

Examples

In the following example, there are two domains, 1 and 2. The output explains that MAP domain 2 is incomplete, and thus it is not active.

```
ciscoasa(config)# show map-domain

MAP Domain 1
  Default Mapping Rule
    IPv6 prefix 2001:db8:cafe:cafe::/64
  Basic Mapping Rule
    IPv6 prefix 2001:cafe:cafe:1::/64
    IPv4 prefix 192.168.3.0 255.255.255.0
    share ratio 16
    start port 1024
    PSID length 4
    PSID offset 6
    Rule EA-bit length 12
MAP Domain 2
  Default Mapping Rule
    IPv6 prefix 2001:db8:1234:1234::/64
Warning: map-domain 2 configuration is incomplete and not in effect.
ciscoasa(config)#
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

show memory

To display a summary of the maximum physical memory and current free memory available to the operating system, use the **show memory** command in privileged EXEC mode.

show memory [**detail**]

Syntax Description

detail	(Optional) Displays a detailed view of free and allocated system memory.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.2(1)	Virtual machine (VMs) statistics were added to the output to support the ASA virtual.
9.3(2)	The internal memory manager has been replaced by the standard glibc library in the **show memory detail** command.

Usage Guidelines

The show memory command lets you display a summary of the maximum physical memory and current free memory available to the operating system. Memory is allocated as needed.

You can also display the information from the show memory command using SNMP.

You can use the **show memory detail** output with the **show memory binsize** command to debug memory leaks.

The show memory detail command output can be broken down into three sections: Summary, DMA Memory, and HEAP Memory. The summary displays the total memory is allocation. Memory that is not tied to DMA or reserved is considered as the HEAP. The Free memory value is the unused memory in the HEAP. The Used memory value indicates the total memory has been allocated. The breakdown of HEAP allocation is displayed later in the output. Reserved memory and DMA Reserved memory are used by different system processes and primarily VPN services.

The Free memory is divided into three parts: Heapcache Pool, Global Shared Pool, and System. Heapcache Pool and Global Shared Pool are the amount of free memory available in the glibc heap. System is the available memory that can be allocated from the underlying system. The total amount of Free memory available to the ASA is the sum of Heapcache Pool, Global Shared Pool, and System.

The Used memory is divided into four parts: Heapcache Pool, Global Shared Pool, Reserved, and System Overhead. Heapcache Pool and Global Shared Pool are the amount of Used memory in the glibc heap. Reserved memory (DMA) is the amount of memory reserved for the DMA pools. System overhead is the glibc overhead and process overhead of various running processes.

- Memory is reserved at boot up for DMA and the heapcache.
- Initially, heap memory is allocated from the heapcache, later from the global shared pool once the heapcache is exhausted.
- The global shared pool receives its memory as needed from the system, and returns freed memory back to the system whenever possible.
- The total free heap memory is inclusive of free memory in the system, plus from the heapcache and the global shared pool.

Values displayed in the allocated memory statistics total (bytes) column do not reflect real values (MEMPOOL_GLOBAL_SHARED POOL STATS) in the **show memory detail** command output.

Note Before Version 9.3(2), all system memory (except what goes in DMA pools) appears as part of MEMPOOL_GLOBAL_SHARED. In other words, all allocatable free memory was in MEMPOOL_GLOBAL_SHARED. As of Version 9.3(2), MEMPOOL_GLOBAL_SHARED doesn't take all the system memory during bootup, but asks the underlying operating system for memory whenever required. Similarly, it returns memory to the system when a significant amount of memory is freed. As a result, the size of MEMPOOL_GLOBAL_SHARED appears to grow and shrink according to demand. A minimal amount of free memory remains in MEMPOOL_GLOBAL_SHARED to speed up allocation.

The output shows that the block of size 49,152 was allocated then returned to the free pool, and another block of size 131,072 was allocated. In this case, you would think that free memory decreased by 131,072-49,152=81,920 bytes, but it actually decreased by 100,000 bytes (see the Free memory line).

```
ciscoasa# show memory detail
Free memory heap:                  1193358928 bytes (13%)
Free memory system:                6596267951 bytes (74%)
Used memory:
     Allocated memory in use:       464188448 bytes ( 5%)
     Reserved memory (DMA):         513802240 bytes ( 6%)
     Memory overhead:               202659216 bytes ( 2%)
-----------------------------   ------------------
Total memory:                      8970276783 bytes (100%)
Least free memory:        7963442431 bytes (89%)
Most used memory:         1006834352 bytes (11%)
MEMPOOL_HEAPCACHE_0 POOL STATS:
Non-mmapped bytes allocated =   1541406720
Number of free chunks       =          633
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =   1541406720
Keepcost                    =   1190961440
Max contiguous free mem     =   1190961440
Allocated memory in use     =    348047792
Free memory                 =   1193358928
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
```

```
                32          177          5664
                48          204          9792
                64          161         10304
                80            3           240
                96            1            96**
               112            2           224
               160            5           800
               192            1           192
               208            1           208
               224            1           224
               240            1           240
               256           13          4064
               384            2           864
               512            3          1648
              1024            1          1296
             12288            1         13792
             24576            2         57424
             32768            1         43824
             65536            1         65616
            262144            1        322672
           1572864            1       1843712
        1190961440            1    1190961440*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
                80         1637        130960
                96        13898       1334208
               112         3422        383264
               128         1910        244480
               144         3677        529488
               160          463         74080
               176          856        150656
               192          357         68544
               208          350         72800
               224          370         82880
               240          337         80880
               256         2293        587008
               384          596        228864
               512          657        336384
               768          504        387072
              1024          449        459776
              1536         1217       1869312
              2048          376        770048
              3072          137        420864
              4096          652       2670592
              6144           73        448512
              8192          212       1736704
             12288          643       7901184
             16384          598       9797632
             24576           31        761856
             32768           77       2523136
             49152           31       1523712
             65536          200      13107200
             98304           30       2949120
            131072           20       2621440
            196608           28       5505024
            262144           14       3670016
            393216           23       9043968
            524288            5       2621440
            786432            9       7077888
           1048576           11      11534336
```

```
      1572864           10       15728640
      2097152            5       10485760
      3145728            3        9437184
      4194304            3       12582912
      6291456            1        6291456
      8388608            1        8388608
     12582912            7       88080384
MEMPOOL_DMA POOL STATS:
Non-mmapped bytes allocated =    513802240
Number of free chunks       =          153
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    513802240
Keepcost                    =    190724944
Max contiguous free mem     =    190724944
Allocated memory in use     =    322994736
Free memory                 =    190807504
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           48           30           1440
           96            1             96**
          112           28           3136
          160            1            160
          208            1            208
          224            1            224
          240            2            480
          256            1            288
          384           19           9104
          512           65          40656
          768            1            800
         1024            2           2608
    190724944            1      190724944*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
          160            1            160
          240           92          22080
          256            2            512
          512            2           1024
         1024          163         166912
         2048            5          10240
         8192            1           8192
        12288           18         221184
        16384            1          16384
        32768           38        1245184
        49152            1          49152
        65536            1          65536
       131072            4         524288
       196608            3         589824
       262144            8        2097152
       393216            6        2359296
       524288            2        1048576
       786432            1         786432
      1048576           11       11534336
      1572864            7       11010048
      3145728            8       25165824
      6291456            5       31457280
      8388608            1        8388608
     12582912            7       88080384
```

```
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =       135168
Number of free chunks       =            4
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        51616
Max contiguous free mem     =        51616
Allocated memory in use     =         4064
Free memory                 =       131104
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
          432            1            432
        40960            1          50848
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           96            1             96
          112            1            112
          160            1            160
          208            3            624
Summary for all pools:
Non-mmapped bytes allocated =   2055344128
Number of free chunks       =          790
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =   2055208960
Keepcost                    =   1381738000
Allocated memory in use     =    671046592
Free memory                 =   1384297536
```

The following output confirms that a block of size 149,0327 was allocated, instead of 131,072:

```
ciscoasa# show memory binsize 131072
MEMPOOL_HEAPCACHE_0 pool bin stats:
pc = 0x7f739a97db9f, size = 1490327  , count = 9
pc = 0x7f7399be30a0, size = 309008   , count = 2
pc = 0x7f7399be31f4, size = 1255704  , count = 9
MEMPOOL_DMA pool bin stats:
pc = 0x7f73984ba38d, size = 323486   , count = 2
pc = 0x7f73984b8e55, size = 320286   , count = 2
MEMPOOL_GLOBAL_SHARED pool bin stats:
```

The approximate number of total bytes shown in the **show memory detail** command output is by design. There are two reasons for this:

- For each fragment size, if you had to get the sum of all fragments, a performance impact would occur because there can be very large number of allocations for a single fragment size and to get the accurate value, you need to walk over thousands of chunks.
- For each binsize, you need to walk through the doubly linked list of allocations and there could be many allocations. In this case, you cannot hog the CPU for an extended period and would need to suspend allocations periodically. After you resume allocations, other processes may have allocated or deallocated memory and memory states may have changed. As a result, the total bytes column gives an approximate value instead of the real value.

Examples

The following is sample output from the **show memory** command:

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

Note: Free memory is the free system memory. Additional memory maybe available from memory pools internal to the ASA process. Use show memory detail command to view this information, but use it carefully since it may cause CPU hogs and packet loss under load.

The following is sample output from the **show memory detail** command:

```
ciscoasa# show memory detail
Heap Memory:
   Free Memory:
      Heapcache Pool:                      447109376 bytes ( 10% )
      Global Shared Pool:                     131152 bytes (  0% )
      System:                             3208100250 bytes ( 72% )
   Used Memory:
      Heapcache Pool:                      257533696 bytes (  6% )
      Global Shared Pool:                       4016 bytes (  0% )
      Reserved (Size of DMA Pool):         234881024 bytes (  5% )
      System Overhead:                     308051968 bytes (  7% )
-------------------------------------     ----------------
   Total Memory:                          4455811482 bytes ( 100% )
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.
-----------------------------------------------------------------------
MEMPOOL_HEAPCACHE_0 POOL STATS:
Non-mmapped bytes allocated =    704643072
Number of free chunks       =          309
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    704643072
Keepcost                    =    446723584
Max contiguous free mem     =    446723584
Allocated memory in use     =    257533696
Free memory                 =    447109376
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           32           91           2912
           48          116           5568
           64           83           5312
           96            1             96**
           96            3            288
          112            1            112
          160            2            320
          224            2            448
          240            1            240
          256            2            544
          384            1            384
          512            2           1392
          768            2           1904
        32768            1          44704
    446723584            1      446723584*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
```

```
----------------  ----------  --------------
              80         937          74960
              96       10758        1032768
             112        2051         229712
             128         898         114944
             144        2887         415728
             160         290          46400
             176         300          52800
             192         164          31488
             208         246          51168
             224         183          40992
             240         208          49920
             256        1396         357376
             384         474         182016
             512         305         156160
             768         322         247296
            1024         240         245760
            1536         321         493056
            2048         171         350208
            3072          45         138240
            4096         259        1060864
            6144          47         288768
            8192         174        1425408
           12288          94        1155072
           16384         571        9355264
           24576          17         417792
           32768          51        1671168
           49152          16         786432
           65536         121        7929856
           98304          14        1376256
          131072           9        1179648
          196608          19        3735552
          262144          12        3145728
          393216          15        5898240
          524288           2        1048576
          786432           9        7077888
         1048576          12       12582912
         1572864           5        7864320
         2097152           3        6291456
         3145728           2        6291456
         4194304           4       16777216
         6291456           3       18874368
         8388608           1        8388608
        12582912           3       37748736
MEMPOOL_DMA POOL STATS:
Non-mmapped bytes allocated =    234881024
Number of free chunks       =          162
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    234881024
Keepcost                    =     90103152
Max contiguous free mem     =     90103152
Allocated memory in use     =    144701888
Free memory                 =     90179136
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
              96           1             96**
             112           1            112
             256          64          20480
             384          32          15360
             512          64          39936
        90103152           1       90103152*
```

```
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
          160            2            320
          256            2            512
          512            1            512
         1024          160         163840
         2048            5          10240
         8192            1           8192
        12288           18         221184
        16384            1          16384
        32768           37        1212416
        49152            2          98304
        65536            1          65536
       131072            4         524288
       196608            2         393216
       262144            4        1048576
       393216            2         786432
       524288            2        1048576
       786432            1         786432
      1048576            3        3145728
      1572864            2        3145728
      3145728            3        9437184
      6291456            2       12582912
     12582912            3       37748736
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =       135168
Number of free chunks       =            4
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =            0
Keepcost                    =        96368
Max contiguous free mem     =        96368
Allocated memory in use     =         4016
Free memory                 =       131152
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
          448            1            448
        20480            1          23296
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           96            1             96
          112            1            112
          160            1            160
          192            3            576
Summary for all pools:
Non-mmapped bytes allocated =    939659264
Number of free chunks       =          475
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    939524096
Keepcost                    =    536923104
Allocated memory in use     =    402239600
Free memory                 =    537419664
On 5585:
========
ciscoasa# show memory
```

```
Free memory:        4544618496 bytes (73%)
Used memory:        1714343936 bytes (27%)
-------------     ------------------
Total memory:       6258962432 bytes (100%)
Note: Free memory is the free system memory. Additional memory may
      be available from memory pools internal to the ASA process.
      Use 'show memory detail' to see this information, but use it
      with care since it may cause CPU hogs and packet loss under load.
ciscoasa# show memory detail
Heap Memory:
   Free Memory:
      Global Shared Pool:                  283589104 bytes (  5% )
      System:                             4544618496 bytes ( 73% )
   Used Memory:
      Global Shared Pool:                   41813520 bytes (  1% )
      Reserved (Size of DMA Pool):         445095936 bytes (  7% )
      System Overhead:                     943845376 bytes ( 15% )
------------------------------------     ----------------
   Total Memory:                          6258962432 bytes ( 100% )
Warning:  The information reported here is computationally expensive to
          determine, and may result in CPU hogs and performance impact.
-----------------------------------------------------------------------
MEMPOOL_DMA POOL STATS:
Non-mmapped bytes allocated =    445095936
Number of free chunks       =          161
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    445095936
Keepcost                    =    250149264
Max contiguous free mem     =    250149264
Allocated memory in use     =    194871536
Free memory                 =    250224400
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           64           1             64
           96           1             96**
          112           1            112
          256          63          20192
          384          32          15360
          512          63          39312
    250149264           1      250149264*
*  - top most releasable chunk.
** - contiguous memory on top of heap.
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
           80           1             80
          144           1            144
          160           2            320
          256           2            512
          512           1            512
         1024         160         163840
         2048           5          10240
         8192           5          40960
        12288          27         331776
        16384           1          16384
        32768          39        1277952
        49152           1          49152
        65536           1          65536
        98304           4         393216
       131072           4         524288
       196608            1        196608
       262144            3        786432
       393216            2        786432
       524288            2       1048576
       786432            5       3932160
      1048576            3       3145728
      1572864            2       3145728
      3145728            4      12582912
     12582912            4      50331648
MEMPOOL_GLOBAL_SHARED POOL STATS:
Non-mmapped bytes allocated =     43286528
Number of free chunks       =          474
Number of mmapped regions   =          156
Mmapped bytes allocated     =    282116096
Max memory footprint        =            0
Keepcost                    =        11200
Max contiguous free mem     =       132816
Allocated memory in use     =     41813520
Free memory                 =      1473008
----- fragmented memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
          32           135          4320
          48           203          9744
          64            38          2432
          80             2           160
          80            20          1600
          96             3           288
          96             3           288
         112            90         10080
         112            10          1120
         128            20          2560
         144             1           144
         240             1           240
         384             1           384
         400             1           400
         448             1           448
         480             1           480
         544             1           544
         560             6          3360
         656             1           656
         816             1           816
         832             1           832
         880             1           880
        1088             3          3360
        1664             1          1680
        3136             1          3280
        3584             1          3776
        8704             1          8704
       24576             1         25728
       40960             1         50064

----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
          64           354         22656
          80          1234         98720
          96         12337       1184352
         112          1202        134624
         128           970        124160
         144          2777        399888
         160           435         69600
```

```
          176           155          27280
          192           323          62016
          208           250          52000
          224            86          19264
          240           388          93120
          256          1478         378368
          384           304         116736
          512           304         155648
          768           314         241152
         1024           410         419840
         1536          1188        1824768
         2048           136         278528
         3072            42         129024
         4096           814        3334144
         6144            56         344064
         8192           174        1425408
        12288           123        1511424
        16384           584        9568256
        24576            30         737280
        32768            60        1966080
        49152            30        1474560
        65536           139        9109504
        98304            25        2457600
       131072            19        2490368
       196608            32        6291456
       262144            18        4718592
       393216            29       11403264
       524288             7        3670016
       786432             8        6291456
      1048576            13       13631488
      1572864            11       17301504
      2097152             6       12582912
      3145728             2        6291456
      4194304             4       16777216
      8388608             1        8388608
     12582912             6       75497472
Summary for all pools:
Non-mmapped bytes allocated =    488382464
Number of free chunks       =          635
Number of mmapped regions   =            0
Mmapped bytes allocated     =    282116096
Max memory footprint        =    445095936
Keepcost                    =    250160464
Allocated memory in use     =    236685056
Free memory                 =    251697408
```

The following is sample output from the **show memory** command on the ASA 5525 after enabling the **jumbo-frame reservation** command and issuing the **write memory** command and the **reload** command:

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
-------------     ------------------
Total memory:       4455811482 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5525 without enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        3208100250 bytes (72%)
Used memory:        1247711232 bytes (28%)
```

```
-------------      ------------------
Total memory:       4455811482 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5515 after enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        3276619472 bytes (76%)
Used memory:        1018347824 bytes (24%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5515 without enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        3481145472 bytes (81%)
Used memory:         813821824 bytes (19%)
-------------       ------------------
Total memory:       4294967296 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5585 after enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        8883297824 bytes (69%)
Used memory:        4001604064 bytes (31%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5585 without enabling the **jumbo-frame reservation** command:

```
ciscoasa# show memory
Free memory:        9872205104 bytes (77%)
Used memory:        3012696784 bytes (23%)
-------------       ------------------
Total memory:      12884901888 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5520, which does not support the **jumbo-frame** command:

```
ciscoasa# show memory
ree memory:         206128232 bytes (38%)
Used memory:         330742680 bytes (62%)
-------------       -----------------
Total memory:        536870912 bytes (100%)
```

The following is sample output from the **show memory** command on the ASA 5505, which does not support the **jumbo-frame** command:

```
ciscoasa# show memory
Free memory:          48457848 bytes (18%)
Used memory:         219977608 bytes (82%)
-------------        -----------------
Total memory:        268435456 bytes (100%
```

The following is sample output from the **show memory** command on the ASA virtual:

```
Free memory:        2694133440 bytes (63%)
Used memory:        1600833856 bytes (37%)
-------------     ------------------
Total memory:       4294967296 bytes (100%)
Virtual platform memory
-----------------------
Provisioned       4096 MB
Allowed           4096 MB
Status            Compliant
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory all

To display a summary of the maximum physical memory and current free memory available to the operating system, use the **show memory all** command in privileged EXEC mode. This value includes lina and snort memory usage.

show memory all

Command History

Release	Modification
9.16(1)	This command was introduced.

Usage Guidelines

The **show memory all** command lets you display a summary of the maximum physical memory and current free memory available to the operating system. Memory is allocated as needed.

```
ciscoasa#show memory all
Data Path:
Free memory:        3161408675 bytes (72%)
Used memory:        1203826208 bytes (28%)
-------------     ------------------
Total memory:       4365234883 bytes (100%)
Inspection Engine:
Free memory:                 0 bytes ( 0%)
Used memory:                 0 bytes ( 0%)
-------------     ------------------
Total memory:                0 bytes (100%)
System:
Free memory:                 0 bytes ( 0%)
Used memory:                 0 bytes ( 0%)
-------------     ------------------
Total memory:                0 bytes (100%)
ciscoasa#
```

show memory api

To display the malloc stack APIs that are registered in the system, use the **show memory api** command in privileged EXEC mode.

show memory api

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays the malloc stack APIs that are registered in the system.

If any of the memory debugging features are turned on (that is, delay-free-poisoner, memory tracker, or memory profiler), their APIs appear in the **show memory api** command output.

Examples

This following is sample output from the **show memory api** command:

```
ciscoasa# show memory api
Resource Manager (0) ->
Tracking (0) ->
Delayed-free-poisoner (0) ->
Core malloc package (0)
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory app-cache

To observe memory usage by application, use the show memory app-cache command in privileged EXEC mode.

show memory app-cache [**threat-detection | host | flow | tcb | http | access-list | tcb-ibs**] [**detail**]

Syntax Description

access-list	(Optional) Shows the application level memory cache for access lists.
detail	(Optional) Shows a detailed view of free and allocated system memory.
flow	(Optional) Shows the application level memory cache for flows.
host	(Optional) Shows application level memory cache for hosts.
http	(Optional) Shows application level memory cache for HTTP.
tcb	(Optional) Shows application level memory cache for TCB.
tcb-ips	(Optional) Shows application level memory cache for TCB-IPS.
threat-detection	(Optional) Shows application level memory cache for threat detection.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(1)	This command was added.
8.1(1)	The **access-list** and **http** options were added.
9.10(1)	The tcb-ips option was added.

Usage Guidelines

This command enables you to observe memory usage by application.

Examples

The following is sample output from the **show memory app-cache threat-detection** command:

```
ciscoasa(config)# show memory app-cache threat-detection
```

```
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

The following is sample output from the **show memory app-cache threat-detection detail** command:

```
ciscoasa(config)# show memory app-cache threat-detection detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
TD ACE stats 50 0 2 0 1936
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host/Port counte 100 0 2 0 48
TD Host stats 50 50 16120 0 116515360
TD Subnet stats 50 2 113 0 207016
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 100 24618 0 3544992
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
TD Host/Port counte 100 2 113 0 5424
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 1350 460 115167 0 130926168
```

The following is sample output from the **show memory app-cache host detail** command:

```
ciscoasa(config)# show memory app-cache host detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Host Core 0 1000 1000 5116 0 961808
SNP Host Core 1 1000 1000 4968 0 933984
SNP Host Core 2 1000 1000 5413 0 1017644
SNP Host Core 3 1000 1000 4573 0 859724
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 20070 0 3773160
```

The following is sample output from the **show memory app-cache flow detail** command:

```
ciscoasa(config)# show memory app-cache flow detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP Conn Core 0 1000 1000 893 0 639388
SNP Conn Core 1 1000 948 980 0 701680
SNP Conn Core 2 1000 1000 1175 0 841300
SNP Conn Core 3 1000 1000 901 0 645116
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 3948 3949 0 2827484
```

The following is sample output from the **show memory app-cache access-list detail** command:

```
ciscoasa(config)# show memory app-cache access-list detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
NP ACL log c Core 0 1000 0 1 0 68
NP ACL log c Core 1 1000 0 6 0 408
NP ACL log c Core 2 1000 0 19 0 1292
NP ACL log c Core 3 1000 0 0 0 0
NP ACL log f Core 0 1000 0 0 0 0
NP ACL log f Core 1 1000 0 0 0 0
NP ACL log f Core 2 1000 0 0 0 0
NP ACL log f Core 3 1000 0 0 0 0
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 26 0 1768
```

The following is sample output from the **show memory app-cache http detail** command:

```
ciscoasa(config)# show memory app-cache http detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
Inspect HTTP Core 0 1000 0 0 0 0
Inspect HTTP Core 1 1000 0 0 0 0
Inspect HTTP Core 2 1000 0 0 0 0
Inspect HTTP Core 3 1000 0 0 0 0
HTTP Result Core 0 1000 0 0 0 0
HTTP Result Core 1 1000 0 0 0 0
HTTP Result Core 2 1000 0 0 0 0
HTTP Result Core 3 1000 0 0 0 0
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 8000 0 0 0 0
```

The following is sample output from the **show memory app-cache tcb detail** command:

```
ciscoasa(config)# show memory app-cache tcb detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB Core 0 1000 1000 968 0 197472
SNP TCB Core 1 1000 1000 694 0 141576
SNP TCB Core 2 1000 1000 1304 0 266016
SNP TCB Core 3 1000 1000 1034 0 210936
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 4000 4000 4000 0 816000
```

The following is sample output from the **show memory app-cache tcb-ips detail** command:

```
ha-asa5512a(config)# show memory app-cache tcb-ips detail
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
SNP TCB IPS Core 00     625 0 0 0 0
LIMIT      COUNT      ALLOC     FAILED   BYTES USED
TOTAL         625          0 0 0            0
ha-asa5512a(config)# show memory app-cache
CACHE NAME LIMIT COUNT ALLOC FAILED BYTES USED
[...]
SNP TCB IPS Core 00 625 0 0 0 0
SNP TCB IPS Total 625 0 0 0 0
[...]
LIMIT COUNT ALLOC FAILED BYTES USED
TOTAL 61972 149 188 0        50212
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.

show memory appcache-threshold

To display the status and hit count of memory appcache-threshold, use the show memory appcache-threshold command in the privileged EXEC mode.

show memory appcache-threshold

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.10(1)	This command was introduced.

Usage Guidelines

Use **show memory appcache-threshold** command to display the hit count and status of memory allocation threshold for a managed application.

Examples

The following example displays the memory appcache threshold status for a managed application:

```
ciscoasa# show memory appcache-threshold
          CACHE NAME   STATUS      THRESHOLD     HIT COUNT
    SNP Conn Core 00   ENABLED            85             5

ciscoasa# show memory appcache-threshold
          CACHE NAME   STATUS      THRESHOLD     HIT COUNT
    SNP Conn Core 00   DISABLED           85             5
```

Table 70: show memory appcache-threshold Fields

Field	Description
Cache Name	The name of the managed application cache. For ASA 9.10.1 release, only the SNP Conn Core 00 application cache type is managed.
Status	Whether the appcache-threshold feature on this application cache type is enabled or disabled.
Threshold	The threshold of this application cache type. For example, 85 means 85% of the system memory used.

Field	Description
Hit Count	The number of times this threshold being hit since the counter was cleared last time.

Related Commands

Command	Description
memory appcache-threshold enable	Enable memory appcache-threshold to restrict application cache allocations after reaching certain memory threshold
clear memory appcache-threshold	Clear the hit count of memory appcache-threshold

show memory binsize

To display summary information about the chunks allocated for a specific bin size, use the **show memory binsize** command in privileged EXEC mode.

show memory binsize *size*

Syntax Description

size	Displays chunks (memory blocks) of a specific bin size. The bin size is from the "fragment size" column of the **show memory detail** command output.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example displays summary information about a chunk allocated to a bin size of 500:

```
ciscoasa# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

Related Commands

Command	Description
show memory-caller address	Displays the address ranges configured on the ASA.
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory	Displays a summary of the maximum physical memory and current free memory available to the operating system.

show memory caller-address

To display the address ranges configured on the ASA, use the **show memory caller-address** command in privileged EXEC mode.

show memory caller-address

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

You must first configure an address ranges with the **memory caller-address** command before you can display them with the **show memory-caller address** command.

Examples

The following examples show how to configure the address ranges with the **memory caller-address** command, and the resulting output of the **show memory-caller address** command:

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08
ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14
ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

If address ranges are not configured before entering the **show memory-caller address** command, no addresses display:

```
ciscoasa# show memory-caller address
Move down stack frame for the addresses:
```

Related Commands

Command	Description
memory caller-address	Configures a block of memory for the caller PC.

show memory delayed-free-poisoner

To display a summary of the **memory delayed-free-poisoner** queue usage, use the **show memory delayed-free-poisoner** command in privileged EXEC mode.

show memory delayed-free-poisoner

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **clear memory delayed-free-poisoner** command to clear the queue and statistics.

Examples

This following is sample output from the **show memory delayed-free-poisoner** command:

```
ciscoasa# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
   3335600:  memory held in queue
      6095:  current queue count
         0:  elements dequeued
         3:  frees ignored by size
      1530:  frees ignored by locking
        27:  successful validate runs
         0:  aborted validate runs
  01:09:36:  local time of last validate
```

Table 9-11 describes the significant fields in the **show memory delayed-free-poisoner** command output.

Table 71: show memory delayed-free-poisoner Command Output Descriptions

Field	Description
memory held in queue	The memory that is held in the delayed free-memory poisoner tool queue. Such memory is normally in the "Free" quantity in the **show memory** output if the delayed free-memory poisoner tool is not enabled.
current queue count	The number of elements in the queue.
elements dequeued	The number of elements that have been removed from the queue. This number begins to increase when most or all of the otherwise free memory in the system ends up in being held in the queue.
frees ignored by size	The number of free requests not placed into the queue because the request was too small to hold required tracking information.
frees ignored by locking	The number of free requests intercepted by the tool not placed into the queue because the memory is in use by more than one application. The last application to free the memory back to the system ends up placing such memory regions into the queue.
successful validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that the queue contents were validated (either automatically or by the **memory delayed-free-poisoner validate** command).
aborted validate runs	The number of times since monitoring was enabled or cleared using the **clear memory delayed-free-poisoner** command that requests to check the queue contents have been aborted because more than one task (either the periodic run or a validate request from the CLI) attempted to use the queue at a time.
local time of last validate	The local system time when the last validate run completed.

Related Commands

Command	Description
clear memory delayed-free-poisoner	Clears the delayed free-memory poisoner tool queue and statistics.
memory delayed-free-poisoner enable	Enables the delayed free-memory poisoner tool.
memory delayed-free-poisoner validate	Forces validation of the elements in the delayed free-memory poisoner tool queue.

show memory logging

To display the memory usage for logging, use the **show memory logging** command in privileged EXEC mode.

show memory logging [**brief | wrap | include** [**address**] [**caller**] [**operator**] [**size**] [**process**] [**time**] [**context**]]

Syntax Description

address	(Optional) Displays address information.
brief	(Optional) Displays abbreviated memory usage logging.
caller	(Optional) Displays caller information.
context	(Optional) Displays virtual context information.
include	Includes only the specified fields in the output. You can specify the fields in any order, but they always appear in the following order: **1.** Process **2.** Time **3.** Context (unless in single mode) **4.** Operation (free/malloc/etc.) **5.** Address **6.** Size **7.** Callers The output format is: process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX Up to four caller addresses appear. The types of operations are listed in the output (Number of...) shown in the example.
operator	(Optional) Displays operator information.
process	(Optional) Displays process information.
size	(Optional) Displays size information.
time	(Optional) Displays time information.
wrap	(Optional) Displays memory usage logging wrapped data, which is purged after you enter this command so that duplicate data does not appear and is not saved.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.4(1)	This command was introduced.

Usage Guidelines

The show memory logging command shows log memory allocations and memory usage, and lets you respond to memory logging wrap events.

Examples

```
The following is sample output from the show memory logging
command on the ASA:
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542 0x0000000000bfef9a

0x0000000000bff606 process=[CMGR Server Process] time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098 0x000000000182c08d

0x000000000182c262 process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b 0x000000000182c08d
```

```
0x000000000182c262 process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542 0x000000000182774d

0x000000000182cc8a process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542 0x0000000000bfef9a

0x0000000000bff606 process=[CMGR Server Process] time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542 0x000000000131911a

0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b
```

The following is sample output from the **show memory logging include process operation size** command on the ASA:

```
ciscoasa# show memory logging include process operation size
Number of free                        6
Number of calloc                      0
Number of malloc                      8
Number of realloc-new                 0
Number of realloc-free                0
Number of realloc-null                0
Number of realloc-same                0
Number of calloc-fail                 0
Number of malloc-fail                 0
Number of realloc-fail                0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free] size=72 process=
[CMGR Server Process] oper=[malloc] size=16 process=[CMGR Server Process] oper=[malloc]
size=512 process=[CMGR Server Process] oper=[free] size=512 process=[CMGR Server Process]
oper=[malloc] size=40 process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server

Process] oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16 process=[CMGR

Server Process] oper=[malloc] size=512 process=[CMGR Server Process] oper=[free] size=512
process=[CMGR Server Process] oper=[malloc] size=40 process=[ci/console] oper=[malloc]
size=72
process=[ci/console] oper=[free] size=72
```

The following is sample output from the **show memory logging brief** command on the ASA:

```
ciscoasa# show memory logging brief
Number of free                        6
Number of calloc                      0
Number of malloc                      8
Number of realloc-new                 0
Number of realloc-free                0
Number of realloc-null                0
Number of realloc-same                0
Number of calloc-fail                 0
Number of malloc-fail                 0
Number of realloc-fail                0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

Related Commands

Command	Description
show memory profile	Displays information about the memory usage (profiling) of the ASA.
show memory binsize	Displays summary information about the chunks allocated for a specific bin size.

show memory profile

To display information about the memory usage (profiling) of the ASA, use the **show memory profile** command in privileged EXEC mode.

show memory profile [**peak**] [**detail | collated | status**]

Syntax Description

collated	(Optional) Collates the memory information displayed.
detail	(Optional) Displays detailed memory information.
peak	(Optional) Displays the peak capture buffer rather than the "in use" buffer.
status	(Optional) Displays the current state of memory profiling and the peak capture buffer.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **show memory profile** command to troubleshoot memory usage level and memory leaks. You can still see the profile buffer contents even if profiling has been stopped. Starting profiling clears the buffer automatically.

Note The ASA might experience a temporary reduction in performance when memory profiling is enabled.

Examples

The following is sample output from the **show memory profile** command:

```
ciscoasa# show memory profile

Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

The output of the **show memory profile detail** command is divided into six data columns and one header column, at the far left. The address of the memory bucket corresponding to the first data column is given at the header column (the hexadecimal number). The data itself is the number of bytes that is held by the text/code that falls in the bucket address. A period (.) in the data column means no memory is held by the text at this bucket. Other columns in the row correspond to the bucket address that is greater than the increment amount from the previous column. For example, the address bucket of the first data column in the first row is 0x001069e0. The address bucket of the second data column in the first row is 0x001069e4 and so on. Normally the header column address is the next bucket address; that is, the address of the last data column of the previous row plus the increment. All rows without any usage are suppressed. More than one such contiguous row can be suppressed, indicated with three periods at the header column (...).

The following is sample output from the **show memory profile detail** command:

```
ciscoasa# show memory profile detail

Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
<snip>
```

The following is sample output from the **show memory profile collated** command:

```
ciscoasa# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
<More>
```

The following is sample output from the **show memory profile peak** command, which shows the peak capture buffer:

```
ciscoasa# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004 Total = 102400
```

The following is sample output from the **show memory profile peak detail** command, which shows the peak capture buffer and the number of bytes that is held by the text/code that falls in the corresponding bucket address:

```
ciscoasa# show memory profile peak detail

Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

The following is sample output from the **show memory profile status** command, which shows the current state of memory profiling and the peak capture buffer:

```
ciscoasa# show memory profile status

InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a program text range of memory to profile.
clear memory profile	Clears the memory buffers held by the memory profiling function.

show memory region

To show the processes maps, use the **show memory region** command in privileged EXEC mode.

show memory region

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **show memory region** command shows the processes memory map.

Examples

The following is sample output from the **show memory region** command:

```
ciscoasa# show memory region
ASLR enabled, text region 7f7397701000-7f739bc186c4
Address Perm Offset Dev Inode Pathname
7f7391a06000-7f7391d09000 rw-p 00000000 00:00 0 [stack:2161]
7f7391d2a000-7f739212e000 rw-p 00000000 00:00 0 [stack:2157]
7f7392530000-7f7392631000 rw-p 00000000 00:00 0 [stack:2156]
7f7392647000-7f7392849000 rw-p 00000000 00:00 0 [stack:2154]
7f7392895000-7f7392897000 r-xp 00000000 00:01 989 /lib64/libutil-2.18.so
7f7392897000-7f7392a96000 ---p 00002000 00:01 989 /lib64/libutil-2.18.so
7f7392a96000-7f7392a97000 r--p 00001000 00:01 989 /lib64/libutil-2.18.so
7f7392a97000-7f7392a98000 rw-p 00002000 00:01 989 /lib64/libutil-2.18.so
7f7392a98000-7f7392c9a000 r-xp 00000000 00:01 2923 /usr/lib64/libcrypto.so.1.0.0
7f7392c9a000-7f7392e99000 ---p 00202000 00:01 2923 /usr/lib64/libcrypto.so.1.0.0
```

```
7f7392e99000-7f7392ec3000 rw-p 00201000 00:01 2923 /usr/lib64/libcrypto.so.1.0.0
7f7392ec7000-7f7392f28000 r-xp 00000000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7392f28000-7f7393127000 ---p 00061000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7393127000-7f7393132000 rw-p 00060000 00:01 3114 /usr/lib64/libssl.so.1.0.0
7f7393132000-7f739316a000 r-xp 00000000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739316a000-7f739336a000 ---p 00038000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739336a000-7f739336c000 rw-p 00038000 00:01 3202 /usr/lib64/libxslt.so.1.1.28
7f739336c000-7f73933ca000 r-xp 00000000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73933ca000-7f73935ca000 ---p 0005e000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73935ca000-7f73935ce000 rw-p 0005e000 00:01 3439 /usr/lib64/libxmlsec1.so.1.2.20
7f73935ce000-7f7393606000 r-xp 00000000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393606000-7f7393805000 ---p 00038000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f7393805000-7f7393809000 rw-p 00037000 00:01 2950 /usr/lib64/libxmlsec1-openssl.so.1.2.20
7f739380a000-7f7393811000 r-xp 00000000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393811000-7f7393a11000 ---p 00007000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393a11000-7f7393a12000 rw-p 00007000 00:01 2976 /usr/lib64/libffi.so.6.0.1
7f7393a12000-7f7393b94000 r-xp 00000000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393b94000-7f7393d94000 ---p 00182000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393d94000-7f7393dd3000 rw-p 00182000 00:01 2929 /usr/lib64/libpython2.7.so.1.0
7f7393de1000-7f7393df6000 r-xp 00000000 00:01 948 /lib64/libz.so.1.2.8
7f7393df6000-7f7393ff5000 ---p 00015000 00:01 948 /lib64/libz.so.1.2.8
7f7393ff5000-7f7393ff6000 rw-p 00014000 00:01 948 /lib64/libz.so.1.2.8
7f7393ff6000-7f739419a000 r-xp 00000000 00:01 961 /lib64/libc-2.18.so
7f739419a000-7f7394399000 ---p 001a4000 00:01 961 /lib64/libc-2.18.so
7f7394399000-7f739439d000 r--p 001a3000 00:01 961 /lib64/libc-2.18.so
7f739439d000-7f739439f000 rw-p 001a7000 00:01 961 /lib64/libc-2.18.so
7f73943a3000-7f73943b8000 r-xp 00000000 00:01 949 /lib64/libgcc_s.so.1
7f73943b8000-7f73945b8000 ---p 00015000 00:01 949 /lib64/libgcc_s.so.1
7f73945b8000-7f73945b9000 rw-p 00015000 00:01 949 /lib64/libgcc_s.so.1
7f73945b9000-7f73946bb000 r-xp 00000000 00:01 999 /lib64/libm-2.18.so
7f73946bb000-7f73948ba000 ---p 00102000 00:01 999 /lib64/libm-2.18.so
7f73948ba000-7f73948bb000 r--p 00101000 00:01 999 /lib64/libm-2.18.so
7f73948bb000-7f73948bc000 rw-p 00102000 00:01 999 /lib64/libm-2.18.so
7f73948bc000-7f73948be000 r-xp 00000000 00:01 3641 /asa/lib/libplatcap.so
```

```
7f73948be000-7f7394abd000 ---p 00002000 00:01 3641 /asa/lib/libplatcap.so
7f7394abd000-7f7394ac5000 rw-p 00001000 00:01 3641 /asa/lib/libplatcap.so
7f7394ac5000-7f7394b12000 r-xp 00000000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394b12000-7f7394d12000 ---p 0004d000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d12000-7f7394d14000 rw-p 0004d000 00:01 3213 /usr/lib64/libgobject-2.0.so.0.3600.4
7f7394d14000-7f7394e3d000 r-xp 00000000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f7394e3d000-7f739503d000 ---p 00129000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f739503d000-7f739503f000 rw-p 00129000 00:01 3120 /usr/lib64/libglib-2.0.so.0.3600.4
7f739503f000-7f73950ce000 r-xp 00000000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73950ce000-7f73952ce000 ---p 0008f000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73952ce000-7f73952d9000 rw-p 0008f000 00:01 3143 /usr/lib64/liblasso.so.3.11.1
7f73952d9000-7f73952e9000 r-xp 00000000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73952e9000-7f73954e8000 ---p 00010000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e8000-7f73954e9000 rw-p 0000f000 00:01 3175 /usr/lib64/libprotobuf-c.so.0.0.0
7f73954e9000-7f739551b000 r-xp 00000000 00:01 3629 /asa/lib/libmsglyr.so
7f739551b000-7f739571b000 ---p 00032000 00:01 3629 /asa/lib/libmsglyr.so
7f739571b000-7f7395720000 rw-p 00032000 00:01 3629 /asa/lib/libmsglyr.so
7f7395720000-7f739576c000 r-xp 00000000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f739576c000-7f739596c000 ---p 0004c000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f739596c000-7f7395970000 rw-p 0004c000 00:01 3146 /usr/lib64/libzmq.so.3.1.0
7f7395970000-7f7395ac0000 r-xp 00000000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395ac0000-7f7395cc0000 ---p 00150000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395cc0000-7f7395cca000 rw-p 00150000 00:01 2952 /usr/lib64/libxml2.so.2.9.1
7f7395ccb000-7f7395ceb000 r-xp 00000000 00:01 3628 /asa/lib/libpdts.so
7f7395ceb000-7f7395eea000 ---p 00020000 00:01 3628 /asa/lib/libpdts.so
7f7395eea000-7f7395eec000 rw-p 0001f000 00:01 3628 /asa/lib/libpdts.so
7f7395eec000-7f7395eff000 r-xp 00000000 00:01 2057 /lib64/libresolv-2.18.so
7f7395eff000-7f73960ff000 ---p 00013000 00:01 2057 /lib64/libresolv-2.18.so
7f73960ff000-7f7396100000 r--p 00013000 00:01 2057 /lib64/libresolv-2.18.so
7f7396100000-7f7396101000 rw-p 00014000 00:01 2057 /lib64/libresolv-2.18.so
7f7396103000-7f7396110000 r-xp 00000000 00:01 955 /lib64/libudev.so.0.13.1
7f7396110000-7f739630f000 ---p 0000d000 00:01 955 /lib64/libudev.so.0.13.1
7f739630f000-7f7396310000 rw-p 0000c000 00:01 955 /lib64/libudev.so.0.13.1
7f7396310000-7f7396322000 r-xp 00000000 00:01 964 /lib64/libcgroup.so.1.0.38
```

```
7f7396322000-7f7396521000 ---p 00012000 00:01 964 /lib64/libcgroup.so.1.0.38
7f7396521000-7f7396523000 rw-p 00011000 00:01 964 /lib64/libcgroup.so.1.0.38
7f739677d000-7f7396784000 r-xp 00000000 00:01 2067 /lib64/librt-2.18.so
7f7396784000-7f7396983000 ---p 00007000 00:01 2067 /lib64/librt-2.18.so
7f7396983000-7f7396984000 r--p 00006000 00:01 2067 /lib64/librt-2.18.so
7f7396984000-7f7396985000 rw-p 00007000 00:01 2067 /lib64/librt-2.18.so
7f7396985000-7f7396988000 r-xp 00000000 00:01 2060 /lib64/libdl-2.18.so
7f7396988000-7f7396b87000 ---p 00003000 00:01 2060 /lib64/libdl-2.18.so
7f7396b87000-7f7396b88000 r--p 00002000 00:01 2060 /lib64/libdl-2.18.so
7f7396b88000-7f7396b89000 rw-p 00003000 00:01 2060 /lib64/libdl-2.18.so
7f7396b89000-7f7396ba2000 r-xp 00000000 00:01 1001 /lib64/libpthread-2.18.so
7f7396ba2000-7f7396da1000 ---p 00019000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da1000-7f7396da2000 r--p 00018000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da2000-7f7396da3000 rw-p 00019000 00:01 1001 /lib64/libpthread-2.18.so
7f7396da7000-7f7396dce000 r-xp 00000000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396dce000-7f7396fcd000 ---p 00027000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396fcd000-7f7396fd0000 rw-p 00026000 00:01 3434 /usr/lib64/libexpat.so.1.6.0
7f7396fd0000-7f73970b6000 r-xp 00000000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73970b6000-7f73972b5000 ---p 000e6000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972b5000-7f73972bd000 r--p 000e5000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972bd000-7f73972bf000 rw-p 000ed000 00:01 3113 /usr/lib64/libstdc++.so.6.0.18
7f73972d4000-7f73972de000 r-xp 00000000 00:01 3174 /usr/lib64/libnuma.so.1
7f73972de000-7f73974dd000 ---p 0000a000 00:01 3174 /usr/lib64/libnuma.so.1
7f73974dd000-7f73974de000 rw-p 00009000 00:01 3174 /usr/lib64/libnuma.so.1
7f73974de000-7f73974fe000 r-xp 00000000 00:01 950 /lib64/ld-2.18.so
7f73976fe000-7f73976ff000 r--p 00020000 00:01 950 /lib64/ld-2.18.so
7f73976ff000-7f7397700000 rw-p 00021000 00:01 950 /lib64/ld-2.18.so
7f7397701000-7f739bc19000 r-xp 00000000 00:01 3650 /asa/bin/lina
7f739be18000-7f739cc16000 rw-p 04517000 00:01 3650 /asa/bin/lina
7ffffe1fc000-7ffffe21d000 rw-p 00000000 00:00 0 [stack]
7ffffe2f1000-7ffffe2f3000 r-xp 00000000 00:00 0 [vdso]
```

Related Commands

Command	Description
memory profile enable	Enables the monitoring of memory usage (memory profiling).
memory profile text	Configures a program text range of memory to profile.
clear memory profile	Clears the memory buffers held by the memory profiling function.

show memory top-usage

To display the top number of allocated fragment sizes from the **show memory detail** command, use the **show memory top-usage** command in privileged EXEC mode.

show memory top-usage [*num*]

Syntax Description

num	(Optional) Shows the number of bin sizes to list. Valid values are from 1-64.

Command Default

The default for *num* is 10.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(6)	This command was added.

Usage Guidelines

Use the **show memory top-usage** command to display the top number of allocated fragment sizes from the **show memory detail** command.

This command does not use clustering and does not need to be disabled when clustering is enabled.

Examples

The following is sample output from the show memory top-usage command:

```
ciscoasa# show memory top-usage 3
MEMPOOL_DMA pool binsize allocated byte totals:
----- allocated memory statistics -----
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
      1572864            9       14155776
     12582912            1       12582912
      6291456            1        6291456
----- Binsize PC top usage -----
Binsize: 1572864                total (bytes): 14155776
pc = 0x805a870, size = 16422399 , count = 9
Binsize: 12582912               total (bytes): 12582912
pc = 0x805a870, size = 12960071 , count = 1
Binsize: 6291456                total (bytes): 6291456
pc = 0x9828a6c, size = 7962695  , count = 1
MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:
----- allocated memory statistics -----
```

```
 fragment size       count          total
    (bytes)                        (bytes)
----------------  ----------  --------------
     12582912            1       12582912
      2097152            6       12582912
        65536          181       11862016
----- Binsize PC top usage -----
Binsize: 12582912              total (bytes): 12582912
pc = 0x8249763, size = 37748736 , count = 1
Binsize: 2097152               total (bytes): 12582912
pc = 0x8a7ebfb, size = 2560064  , count = 1
pc = 0x8aa4413, size = 2240064  , count = 1
pc = 0x8a9bb13, size = 2240064  , count = 1
pc = 0x8a80542, size = 2097152  , count = 1
pc = 0x97e7172, size = 2097287  , count = 1
pc = 0x8996463, size = 2272832  , count = 1
Binsize: 65536                 total (bytes): 11862016
pc = 0x913db2b, size = 11635232 , count = 161
pc = 0x91421eb, size = 138688   , count = 2
pc = 0x97e7172, size = 339740   , count = 4
pc = 0x97e7433, size = 197229   , count = 3
pc = 0x82c3412, size = 65536    , count = 1
pc = 0x8190e09, size = 155648   , count = 2
pc = 0x8190af6, size = 77824    , count = 1
pc = 0x93016a1, size = 65536    , count = 1
pc = 0x89f1a40, size = 65536    , count = 1
pc = 0x9131140, size = 163968   , count = 2
pc = 0x8ee56c8, size = 66048    , count = 1
pc = 0x8056a01, size = 66528    , count = 1
pc = 0x80569e5, size = 66528    , count = 1
```

Related Commands

Command	Description
show memory tracking	Shows all currently collected information.

show memory tracking

To display currently allocated memory tracked by the tool, use the **show memory tracking** command in privileged EXEC mode.

show memory tracking [**address** | **dump** | **detail**]

Syntax Description

address	(Optional) Shows memory tracking by address.
detail	(Optional) Shows the internal memory tracking state.
dump	(Optional) Shows the memory tracking address.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use the **show memory tracking** command to show currently allocated memory tracked by the tool.

Examples

The following is sample output from the show memory tracking command:

```
ciscoasa# show memory tracking
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
```

The following is sample output from the show memory tracking address command:

```
ciscoasa# show memory tracking address
memory tracking by caller:
17 bytes from 1 allocates by 0x080c50c2
37 bytes from 1 allocates by 0x080c50f6
57 bytes from 1 allocates by 0x080c5125
20481 bytes from 1 allocates by 0x080c5154
memory tracking by address:
```

```
37 byte region @ 0xa893ae80 allocated by 0x080c50f6
57 byte region @ 0xa893aed0 allocated by 0x080c5125
20481 byte region @ 0xa8d7cc50 allocated by 0x080c5154
17 byte region @ 0xa8a6f370 allocated by 0x080c50c2
```

The following is sample output from the show memory tracking dump command:

```
ciscoasa# show
 memory tracking dump
Tracking data for the 57 byte region at 0xa893aed0:
Timestamp: 05:59:36.309 UTC Sun Jul 29 2007
Traceback:
0x080c5125
0x080b3695
0x0873f606
0x08740573
0x080ab530
0x080ac788
0x080ad141
0x0805df8f
Dumping 57 bytes of the 57 byte region:
a893aed0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aee0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893aef0: 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c 0c | ................
a893af00: 0c 0c 0c 0c 0c 0c 0c 0c 0c | .........
```

Related Commands

Command	Description
clear memory tracking	Clears all currently collected information.

show memory utilization

Use the show memory utilization command to view the configured reload threshold limit and the crash information on ASA.

show memory-utilization [**reload-threshold**]

Syntax Description

reload-threshold	Displays the configured system memory reload threshold limit, and if crash information is saved before a system reload.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

Use the **show memory utilization** command to know if a reload threshold is configured. If configured, you can view the threshold limit and whether the optional choice to save crash information before a reload is set.

Examples

The following example displays how to configure memory utilization feature on ASA:

```
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is not configured.
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 93%
Crashinfo Generation: yes
ciscoasa# show memory-utilization reload-threshold
Memory-Utilization reload-threshold is configured:
Reload at: 90%
Crashinfo Generation: no
```

show memory webvpn

To generate memory usage statistics for WebVPN, use the **show memory webvpn** command in privileged EXEC mode.

show memory webvpn [**allobjects | blocks | dumpstate** [**cache | disk0 | disk1 | flash | ftp | system | tftp**] **| pools | profile** [**clear | dump | start | stop**] **| usedobjects** { { **begin | exclude | grep | include** } **line** *line* }]

Syntax Description

allobjects	Displays WebVPN memory consumption details for pools, blocks , and all used and freed objects.
begin	Begins with the line that matches.
blocks	Displays WebVPN memory consumption details for memory blocks.
cache	Specifies a filename for a WebVPN memory cache state dump.
clear	Clears the WebVPN memory profile.
disk0	Specifies a filename for WebVPN memory disk0 state dump.
disk1	Specifies a filename for WebVPN memory disk1 state dump:.
dump	Puts WebVPN memory profile into a file.
dumpstate	Puts WebVPN memory state into a file.
exclude	Excludes the line(s) that match.
flash	Specifies a filename for the WebVPN memory flash state dump.
ftp	Specifies a filename for the WebVPN memory FTP state dump.
grep	Includes or excludes lines that match.
include	Includes the line(s) that match.
line	Identifies the line(s) to match.
line	Specifies the line(s) to match.
pools	Shows WebVPN memory consumption details for memory pools.
profile	Obtains the WebVPN memory profile and places it in a file.
system	Specifies a filename for the WebVPN memory system state dump.
start	Starts gathering the WebVPN memory profile.
stop	Stops getting the WebVPN memory profile.
tftp	Specifies a filename for a WebVPN memory TFTP state dump.

usedobjects	Displays WebVPN memory consumption details for used objects.

Command Default

No default behavior or value.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—
Global configuration	• Yes	—	• Yes	—	—
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Examples

The following is sample output from the **show memory webvpn allobjects** command:

```
ciscoasa
#
 show memory webvpn
           allobjects

Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

Related Commands

Command	Description
memory-size	Sets the amount of memory on the ASA that WebVPN services can use.

show mfib

To display MFIB in terms of forwarding entries and interfaces, use the **show mfib** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] [**verbose**] [**cluster**]

Syntax Description

cluster	(Optional) Displays the MFIB epoch number and the current timer value.
group	(Optional) Displays the IP address of the multicast group.
source	(Optional) Displays the IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.
verbose	(Optional) Displays additional information about the entries.

Command Default

Without the optional arguments, information for all groups is shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	The **cluster** keyword was added. Applies to the ASA 5580 and 5585-X only.

Examples

The following is sample output from the **show mfib** command:

```
ciscoasa# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib verbose	Displays detail information about the forwarding entries and interfaces.

show mfib active

To display active multicast sources, use the **show mfib active** command in user EXEC or privileged EXEC mode.

show mfib [*group*] **active** [*kbps*]

Syntax Description

group	(Optional) IP address of the multicast group.
kbps	(Optional) Limits the display to multicast streams that are greater-than or equal to this value.

This command has no arguments or keywords.

Command Default

The default value for *kbps* is 4. If a *group* is not specified, all groups are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The output for the show mfib active command displays either positive or negative numbers for the rate PPS. The ASA displays negative numbers when RPF packets fail or when the router observes RPF packets with an interfaces out (OIF) list. This type of activity may indicate a multicast routing problem.

Examples

The following is sample output from the **show mfib active** command:

```
ciscoasa# show mfib active
Active IP Multicast Sources - sending >= 4 kbps
Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)
Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)
Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Related Commands

Command	Description
show mroute active	Displays active multicast streams.

show mfib count

To display MFIB route and packet count data, use the **show mfib count** command in user EXEC or privileged EXEC mode.

show mfib [*group* [*source*]] **count**

Syntax Description

group	(Optional) IP address of the multicast group.
source	(Optional) IP address of the multicast route source. This is a unicast IP address in four-part dotted-decimal notation.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays packet drop statistics.

Examples

The following sample output from the **show mfib count** command:

```
ciscoasa# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

Related Commands

Command	Description
clear mfib counters	Clears MFIB router packet counters.

Command	Description
show mroute count	Displays multicast route counters.

show mfib interface

To display packet statistics for interfaces that are related to the MFIB process, use the **show mfib interface** command in user EXEC or privileged EXEC mode.

show mfib interface [*interface*]

Syntax Description

interface	(Optional) Interface name. Limits the display to the specified interface.

Command Default

Information for all MFIB interfaces is shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example is sample output from the **show mfib interface** command:

```
ciscoasa# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                            [configured,available]
           Ethernet0   up   [        no,       no]
           Ethernet1   up   [        no,       no]
           Ethernet2   up   [        no,       no]
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib reserved

To display reserved groups, use the **show mfib reserved** command in user EXEC or privileged EXEC mode.

show mfib reserved [**count** | **verbose** | **active** [*kpbs*]]

Syntax Description

active	(Optional) Displays active multicast sources.
count	(Optional) Displays packet and route count data.
kpbs	(Optional) Limits the display to active multicast sources greater than or equal to this value.
verbose	(Optional) Displays additional information.

Command Default

The default value for *kbps* is 4.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays MFIB entries in the range 224.0.0.0 through 224.0.0.225.

Examples

The following is sample output from the **show mfib reserved** command:

```
ciscoasa# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
           AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per second/Avg
 Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops Interface Flags: A -
 Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
```

```
outside Flags: IC
dmz Flags: IC
inside Flags: IC
```

Related Commands

Command	Description
show mfib active	Displays active multicast streams.

show mfib status

To display the general MFIB configuration and operational status, use the **show mfib status** command in user EXEC or privileged EXEC mode.

show mfib status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show mfib status** command:

```
ciscoasa# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

show mfib summary

To display summary information about the number of MFIB entries and interfaces, use the **show mfib summary** command in user EXEC or privileged EXEC mode.

show mfib summary

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show mfib summary** command:

```
ciscoasa# show mfib summary
IPv6 MFIB summary:
  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]
  17     total MFIB interfaces
```

Related Commands

Command	Description
show mroute summary	Displays multicast routing table summary information.

show mfib verbose

To display detail information about the forwarding entries and interfaces, use the **show mfib verbose** command in user EXEC or privileged EXEC mode.

show mfib verbose

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show mfib verbose** command:

```
ciscoasa# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

Related Commands

Command	Description
show mfib	Displays MFIB information in terms of forwarding entries and interfaces.

Command	Description
show mfib summary	Displays summary information about the number of MFIB entries and interfaces.

show mgcp

To display MGCP configuration and session information, use the show **mgcp** command in privileged EXEC mode.

show mgcp { **commands | sessions** } [**detail**]

Syntax Description

commands	Lists the number of MGCP commands in the command queue.
detail	(Optional) Lists additional information about each command (or session) in the output.
sessions	Lists the number of existing MGCP sessions.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show mgcp commands** command lists the number of MGCP commands in the command queue. The **show mgcp sessions** command lists the number of existing MGCP sessions. The **detail** option includes additional information about each command (or session) in the output.

Examples

The following are examples of the **show mgcp** command options:

```
ciscoasa# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
ciscoasa#
ciscoasa# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
Gateway IP | host-pc-2
Transaction ID  2052
Endpoint name | aaln/1
Call ID | 9876543210abcdef
Connection ID |
Media IP | 192.168.5.7
Media port | 6058
```

```
ciscoasa#
ciscoasa# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
ciscoasa#
ciscoasa# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
Gateway IP | host-pc-2
Call ID | 9876543210abcdef
Connection ID | 6789af54c9
Endpoint name | aaln/1
Media lcl port  6166
Media rmt IP | 192.168.5.7
Media rmt port  6058
ciscoasa#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug mgcp	Enables MGCP debug information.
inspect mgcp	Enables MGCP application inspection.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show conn	Displays the connection state for different connection types.

show mmp

To display information about existing MMP sessions, use the **show mmp** command in privileged EXEC mode.

show mmp [*address*]

Syntax Description

address	Specifies the IP address of an MMP client/server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(4)	This command was added.

Examples

The following example shows the use of the **show mmp** command to display information about existing MMP sessions:

```
ciscoasa
# show mmp
10.0.0.42
MMP session:: inside:10.0.0.42/5443 outside:172.23.62.204/2442
session-id=71AD3EB1-7BE8-42E0-8DC3-E96E41D4ADD5
data:: rx-bytes=1258, tx-bytes=1258
```

Related Commands

Command	Description
debug mmp	Displays inspect MMP events.
inspect mmp	Configures the MMP inspection engine.
show debug mmp	Displays current debug settings for the MMP inspection module.

show mode

To show the security context mode for the running software image and for any image in Flash memory, use the **show mode** command in privileged EXEC mode.

show mode

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show mode** command. The following example shows the current mode and the mode for the non-running image "image.bin":

```
ciscoasa# show mode flash:/image.bin
Firewall mode: multiple
```

The mode can be multiple or single.

Related Commands

Command	Description
context	Creates a security context in the system configuration and enters context configuration mode.
mode	Sets the context mode to single or multiple.

show module

To show information about a module installed on the ASA, use the **show module** command in user EXEC mode.

show module [*id* | **all**] [**details | recover | log** [**console**]]

Syntax Description

all	(Default) Shows information for all modules.
console	(Optional) Shows console log information for the module.
details	(Optional) Shows additional information, including remote management configuration for modules.
id	Specifies the module ID. For a hardware module, specify the slot number, which can be **0** (for the ASA) or **1** (for an installed module). For a software module, specify one of the following names: • **sfr** —ASA FirePOWER module. • **ips** —IPS module • **cxsc** —ASA CX module
log	(Optional) Shows log information for the module.
recover	(Optional) Shows the settings for the **hw-module** or **sw-module module recover** command.

Command Default

By default, information for all modules is shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	This command was modified to include more detail in the output.
8.2(1)	Information about the SSC is included in the output.
8.2(5)	Information about support for the ASA 5585-X and for the IPS SSP on the ASA 5585-X was added.
8.4(4.1)	Support for the ASA CX module was added.

Release	Modification
8.6(1)	For the ASA 5512-X through ASA 5555-X the **log** and **console** keywords were added; the **ips** device ID was added.
9.1(1)	Support for the ASA CX software module was added by adding the **cxsc** module ID.
9.2(1)	Support for the ASA FirePOWER module, including the **sfr** keyword was added.

Usage Guidelines

This command shows information about the modules installed in the ASA. The ASA itself also appears as a module in the display (in slot 0).

Examples

The following is sample output from the **show module** command. Module 0 is the base device; module 1 is a CSC SSM.

```
ciscoasa# show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0
Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0 (Build#1187)
Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)
Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

The following table describes each field listed in the output.

Table 72: show module Output Fields

Field	Description
Mod	The module number, 0 or 1.
Ports	The number of ports.
Card Type	For the device shown in module 0, the type is the platform model. For the SSM in module 1, the type is the SSM type.
Model	The model number for this module.
Serial No.	The serial number.
MAC Address Range	The MAC address range for interfaces on this SSM or, for the device, the built-in interfaces.
Hw Version	The hardware version.
Fw Version	The firmware version.

Field	Description
Sw Version	The software version.
SSM Application Name	The name of the application running on the SSM.
SSM Application Version	The version of the application running on the SSM.
Status	For the device in module 0, the status is Up Sys. The status of the SSM in module 1 can be any of the following: • Initializing—The SSM is being detected and the control communication is being initialized by the device. • Up—The SSM has completed initialization by the device. • Unresponsive—The device encountered an error while communicating with this SSM. • Reloading—The SSM is reloading. • Shutting Down—The SSM is shutting down. • Down—The SSM is shut down. • Recover—The SSM is attempting to download a recovery image. • No Image Present—The IPS software has not been installed.
Data Plane Status	The current state of the data plane.
Compatibility	The compatibility of the SSM relative to the rest of the device.
Slot	The physical slot number (used only in dual SSP mode).

The output of the **show module details** command varies according to which module is installed. For example, output for the CSC SSM includes fields about components of the CSC SSM software.

The following is generic sample output from the **show module 1 details** command:

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

The following table describes the additional fields in the output.

Table 73: show module details Additional Output Fields

Field	Description
DC address (not shown)	(ASA FirePOWER only). The address of the management center that manages the module.
Mgmt IP addr	Shows the IP address for the module's management interface.
Mgmt Network Mask (not shown)	Shows the subnet mask for the management address.
Mgmt Gateway (not shown)	The gateway for the management address.
Mgmt web ports	Shows the ports configured for the module's management interface.
Mgmt TLS enabled	Shows whether transport layer security is enabled (true or false) for connections to the management interface of the module.

For models that allow you to configure software modules, the **show module** command lists all possible modules. Status information indicates whether one of them is installed.

```
ciscoasa# show module

Mod  Card Type                                    Model              Serial No.
---- -------------------------------------------- ------------------ -----------
   0 ASA 5555-X with SW, 8 GE Data, 1 GE Mgmt     ASA5555            FCH1714J6HP
 ips Unknown                                      N/A                FCH1714J6HP
cxsc Unknown                                      N/A                FCH1714J6HP
 sfr FirePOWER Services Software Module           ASA5555            FCH1714J6HP
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   0 bc16.6520.1dcd to bc16.6520.1dd6  1.0          2.1(9)8      100.8(66)11
 ips bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
cxsc bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A
 sfr bc16.6520.1dcb to bc16.6520.1dcb  N/A          N/A          5.3.1-100
Mod  SSM Application Name           Status           SSM Application Version
---- ------------------------------ ---------------- --------------------------
 ips Unknown                        No Image Present Not Applicable
cxsc Unknown                        No Image Present Not Applicable
 sfr ASA FirePOWER                  Up               5.3.1-100
Mod  Status             Data Plane Status     Compatibility
---- ------------------ --------------------- -------------
   0 Up Sys             Not Applicable
 ips Unresponsive       Not Applicable
cxsc Unresponsive       Not Applicable
 sfr Up                 Up
Mod  License Name   License Status  Time Remaining
---- -------------- --------------- ---------------
 ips IPS Module     Enabled         172 days
```

The following is sample output from the **show module 1 recover** command:

```
ciscoasa# show module 1 recover
Module 1 recover parameters. . .
```

```
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

The following is sample output from the **show module 1 details** command when an SSC is installed:

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5505 Security Services Card
Model: ASA-SSC
Hardware version: 0.1
Serial Number: JAB11370240
Firmware version: 1.0(14)3
Software version: 6.2(1)E2
MAC Address Range: 001d.45c2.e832 to 001d.45c2.e832
App. Name: IPS
App. Status: Up
App. Status Desc:
App. Version: 6.2(1)E2
Data plane Status: Up
Status: Up
Mgmt IP Addr: 209.165.201.29
Mgmt Network Mask: 255.255.224.0
Mgmt Gateway: 209.165.201.30
Mgmt Access List: 209.165.201.31/32
     209.165.202.158/32
     209.165.200.254/24
Mgmt Vlan: 20
```

The following is sample output from the **show module 1 details** command when an IPS SSP is installed in an ASA 5585-X:

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA-SSM-20
Hardware version: V1.0
Serial Number: 12345678
Firmware version: 1.0(7)2
Software version: 4.1(1.1)S47(0.1)
MAC Address Range: 000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status: Up
Status: Up
Mgmt IP addr: 10.89.147.13
Mgmt web ports: 443
Mgmt TLS enabled: true
```

The following is sample output from the **show module all** command when a CXSC SSP is installed in an ASA 5585-X:

```
ciscoasa# show module all
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10     JAF1504CBRM
  1 ASA 5585-X CXSC Security Services Processor-1 ASA5585-SSP-IPS10  JAF1510BLSE
Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 5475.d05b.1d54 to 5475.d05b.1d5f  1.0          2.0(7)0      100.7(14)13
  1 5475.d05b.248c to 5475.d05b.2497  1.0          0.0(0)0      1.0
Mod SSM Application Name           Status           SSM Application Version
```

```
--- ------------------------------ ---------------- --------------------------
  1 CXSC Security Module             Up               1.0
Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

The following is sample output from the **show module 1 details** command when a CXSC SSP is installed in an ASA 5585-X:

```
ciscoasa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model: ASA5585-S10C10-K8
Hardware version:   1.0
Serial Number:      123456789
Firmware version:   1.0(9)0
Software version:   CXSC Security Module Version 1.0
App. name:          CXSC Security Module
App. version:       Version 1.0
Data plane Status:  Up
Status:             Up
HTTP Service:       Up
Activated:          Yes
Mgmt IP addr:       100.0.1.4
Mgmt web port:      8443
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
hw-module module recover	Recovers an module by loading a recovery image from a TFTP server.
hw-module module reset	Shuts down an module and performs a hardware reset.
hw-module module reload	Reloads the module software.
hw-module module shutdown	Closes the module software in preparation for being powered off without losing configuration data.
sw-module	Configures a software module.

show monitor-interface

To display information about the interfaces monitored for failover, use the **show monitor-interface** command in privileged EXEC mode.

show monitor-interface

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.2(2)	IPv6 addresses were added to the output.

Usage Guidelines

Because an interface can have more than one IPv6 address configured on it, only the link-local address is displayed in the **show monitor-interface** command. If both IPv4 and IPv6 addresses are configured on an interface, both addresses appear in the output. If there is no IPv4 address configured on the interface, the IPv4 address in the output appears as 0.0.0.0. If there is no IPv6 address configured on an interface, the address is simply omitted from the output.

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Normal (Waiting)—The interface is up but has not yet received a hello packet from the corresponding interface on the peer unit. Verify that a standby IP address has been configured for the interface and that there is connectivity between the two interfaces.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The interface or VLAN is administratively down.
- No Link—The physical link for the interface is down.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Examples

The following is sample output from the **show monitor-interface** command:

```
ciscoasa# show monitor-interface
This host: Primary - Active
                Interface outside (10.86.94.88): Normal (Waiting)
                Interface management (192.168.1.1): Normal (Waiting)
                Interface failif (0.0.0.0/fe80::223:4ff:fe77:fed): Normal (Waiting)
        Other host: Secondary - Failed
                Interface outside (0.0.0.0): Unknown (Waiting)
                Interface management (0.0.0.0): Unknown (Waiting)
                Interface failif (0.0.0.0): Unknown (Waiting)
```

Related Commands

Command	Description
monitor-interface	Enables health monitoring on a specific interface

show mrib client

To display information about the MRIB client connections, use the **show mrib client** command in user EXEC or privileged EXEC mode.

show mrib client [**filter**] [**name** *client_name*]

Syntax Description

filter	(Optional) Displays client filter. Used to view information about the MRIB flags that each client owns and the flags in which each clients is interested.
name *client_name*	(Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as PIM or IGMP.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **filter** option is used to display the route and interface level flag changes that various MRIB clients have registered. This command option also shows what flags are owned by the MRIB clients.

Examples

The following sample output from the **show mrib client** command using the **filter** keyword:

```
ciscoasa# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
```

```
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

Related Commands

Command	Description
show mrib route	Displays MRIB table entries.

show mrib route

To display entries in the MRIB table, use the **show mrib route** command in user EXEC or privileged EXEC mode.

show mmp [[*source* |*] [*group* [/ *prefix-length*]]]

Syntax Description

*	(Optional) Display shared tree entries.
/*prefix-length*	(Optional) Prefix length of the MRIB route. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
group	(Optional) IP address or name of the group.
source	(Optional) IP address or name of the route source.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets.

In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry. The **show mfib count** command displays global counters independent of the routes.

Examples

The following is sample output from the **show mrib route** command:

```
ciscoasa# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS
(*,224.0.0.0/24) Flags: D
(*,224.0.1.39) Flags: S
(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI
(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A
(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

Related Commands

Command	Description
show mfib count	Displays route and packet count data for the MFIB table.
show mrib route summary	Displays a summary of the MRIB table entries.

show mroute

To display the IPv4 multicast routing table, use the **show mroute** command in privileged EXEC mode.

show mroute [*group* [*source*] | **reserved**] [**active** [*rate*] | **count** | **pruned** | **summary**]

Syntax Description

active *rate*	(Optional) Displays only active multicast sources. Active sources are those sending at the specified *rate* or higher. If the *rate* is not specified, active sources are those sending at a rate of 4 kbps or higher.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
group	(Optional) IP address or name of the multicast group as defined in the DNS hosts table.
pruned	(Optional) Displays pruned routes.
reserved	(Optional) Displays reserved groups.
source	(Optional) Source hostname or IP address.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the multicast routing table.

Command Default

If not specified, the *rate* argument defaults to 4 kbps.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show mroute** command displays the contents of the multicast routing table. The ASA populates the multicast routing table by creating (S,G) and (*,G) entries based on PIM protocol messages, IGMP reports, and traffic. The asterisk (*) refers to all source addresses, the “S” refers to a single source address, and the “G” is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (through RPF).

To view the **mroute** commands in the running configuration, use the **show running-config mroute** command.

Examples

The following is sample output from the **show mroute** command:

```
ciscoasa(config)# show mroute
Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State
(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never
(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

The following fields are shown in the **show mroute** output:

- **Flags** —Provides information about the entry.
  - **D—Dense** . Entry is operating in dense mode.
  - **S—Sparse** . Entry is operating in sparse mode.
  - **B—Bidir Group** . Indicates that a multicast group is operating in bidirectional mode.
  - **s—SSM Group** . Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes.
  - **C—Connected** . A member of the multicast group is present on the directly connected interface.
  - **L—Local** . The ASA itself is a member of the multicast group. Groups are joined locally by the **igmp join-group** command (for the configured group).
  - **I—Received Source Specific Host Report** . Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by IGMP. This flag is set only on the DR.
  - **P—Pruned** . Route has been pruned. The software keeps this information so that a downstream member can join the source.
  - **R—RP-bit set** . Indicates that the (S, G) entry is pointing toward the RP.
  - **F—Register flag** . Indicates that the software is registering for a multicast source.
  - **T—SPT-bit set** . Indicates that packets have been received on the shortest path source tree.
  - **J—Join SPT** . For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the ASA to join the source tree.

For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the ASA monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

Note The ASA measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started.

If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the ASA immediately switches to the shortest path source tree when traffic from a new source is received.

- **Timers:Uptime/Expires** —Uptime indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. Expires indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
- **Interface state** —Indicates the state of the incoming or outgoing interface.
  - **Interface** —The interface name listed in the incoming or outgoing interface list.
  - State—Indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold.
- **(*, 239.1.1.40)** and **(* , 239.2.2.1)** —Entries in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source indicates all sources.
- RP—Address of the RP. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
- **Incoming interface** —Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
- **RPF nbr** —IP address of the upstream router to the source.
- **Outgoing interface list** —Interfaces through which packets will be forwarded.

Related Commands

Command	Description
clear configure mroute	Removes the **mroute** commands from the running configuration.
mroute	Configures a static multicast route.
show mroute	Displays IPv4 multicast routing table.
show running-config mroute	Displays configured multicast routes.

show n – show o

show nac-policy

To show the NAC policy usage statistics and the assignment of NAC policies to group policies, use the **show nac-policy** command in privileged EXEC mode.

show nac-policy [*nac-policy-name*]

Syntax Description

nac-policy-name	(Optional) Name of the NAC policy for which to display usage statistics.

Command Default

If you do not specify a name, the CLI lists all NAC policy names along with their respective statistics.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example shows the data for the NAC policies named framework1 and framework2:

```
ciscoasa(config)# show nac-policy
nac-policy framework1 nac-framework
  applied session count = 0
  applied group-policy count = 2
  group-policy list:    GroupPolicy2    GroupPolicy1
nac-policy framework2 nac-framework is not in use.
```

The first line of each NAC policy indicates its name and type (nac-framework). The CLI shows the text "is not in use" next to the policy type if the policy is not assigned to any group policies. Otherwise, the CLI displays the usage data for the group policy. Table 10-1 explains the fields in the **show nac-policy** command.

Table 74: show nac-policy Command Fields

Field	Description
applied session count	Cumulative number of VPN sessions to which this ASA applied the NAC policy.
applied group-policy count	Cumulative number of group polices to which this ASA applied the NAC policy.

Field	Description
group-policy list	List of group policies to which this NAC policy is assigned. In this case, the usage of a group policy does not determine whether it appears in this list; if the NAC policy is assigned to a group policy in the running configuration, then the group policy appears in this list.

Related Commands

clear nac-policy	Resets the NAC policy usage statistics.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
show vpn-session_summary.db	Displays the number IPSec, Cisco WebVPN, and NAC sessions.

show nameif

To view the interface name set using the **nameif** command, use the **show nameif** command in privileged EXEC mode.

show nameif [*physical_interface* [*.subinterface*] | *mapped_name* | **zone**]

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	(Optional) Identifies the interface ID, such as **gigabit ethernet0/1** . See the **interface** command for accepted values.
subinterface	(Optional) Identifies an integer between 1 and 4294967293 designating a logical subinterface.
zone	(Optional) Shows the zone names.

Command Default

If you do not specify an interface, the ASA shows all interface names.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	The **zone** keyword was added.

Usage Guidelines

In multiple context mode, if you mapped the interface ID in the **allocate-interface** command, you can only specify the mapped name in a context. The output for this command shows only the mapped name in the Interface column.

Examples

The following is sample output from the **show nameif** command:

```
ciscoasa# show nameif
Interface                Name                     Security
GigabitEthernet0/0       outside                  0
GigabitEthernet0/1       inside                   100
GigabitEthernet0/2       test2                    50
```

See the following output for the **show nameif zone** command:

```
ciscoasa# show nameif zone
Interface                 Name                    zone-name      Security
GigabitEthernet0/0        inside-1                inside-zone     100
GigabitEthernet0/1.21     inside                  inside-zone     100
GigabitEthernet0/1.31     4                                         0
GigabitEthernet0/2        outside                 outside-zone   0
Management0/0             lan                                       0
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
show interface ip brief	Shows the interface IP address and status.

show nat

To display statistics of NAT policies, use the **show nat** command in privileged EXEC mode.

show nat [**interface** *name*] [*ip_addr* [*mask*] | { **object | object-group** } *name*] [**translated** [**interface** *name*] { *ip_addr* [*mask*] | { **object | object-group** } *name* }] [**detail**]

Syntax Description

detail	(Optional) Includes more verbose expansion of the object fields.
interface *name*	(Optional) Specifies the source interface.
ip_addr [*mask*]	(Optional) Specifies an IP address and subnet mask.
object *name*	(Optional) Specifies a network object or service object.
object-group *name*	(Optional) Specifies a network object group
translated	(Optional) Specifies the translated parameters.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.0(1)	Support for IPv6 traffic, as well as translations between IPv4 and IPv6 were added.

Usage Guidelines

Use the **show nat** command to show runtime representation of the NAT policy. Use the **detail** optional keyword to expand the object and view the object values. Use the additional selector fields to limit the **show nat** command output.

Examples

The following is sample output from the **show nat** command:

```
ciscoasa# show nat
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0

   Manual NAT Policies (Section 3)
   1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
ciscoasa# show nat detail
   Manual NAT Policies (Section 1)
   1 (any) to (any) source dynamic S S' destination static D' D
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.2/32, Mapped: 2.2.2.3/32
       Destination - Real: 10.10.10.0/24, Mapped: 20.20.20.0/24

   Auto NAT Policies (Section 2)
   1 (inside) to (outside) source dynamic A 2.2.2.2
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 1.1.1.1/32, Mapped: 2.2.2.2/32

   Manual NAT Policies (Section 3)
 1 (any) to (any) source dynamic C C' destination static B' B service R R'
       translate_hits = 0, untranslate_hits = 0
       Source - Real: 11.11.11.10-11.11.11.11, Mapped: 192.168.10.10/32
       Destination - Real: 192.168.1.0/24, Mapped: 10.75.1.0/24
       Service - Real: tcp source eq 10 destination eq ftp-data , Mapped: tcp source eq
       100 destination eq 200
```

The following is sample output from the **show nat detail** command between IPv6 and IPv4:

```
ciscoasa# show nat detail
1 (in) to (outside) source dynamic inside_nw outside_map destination static inside_map any
translate_hits = 0, untranslate_hits = 0
Source - Origin: 2001::/96, Translated: 192.168.102.200-192.168.102.210
Destination - Origin: 2001::/96, Translated: 0.0.0.0/0
```

Starting with version 9.16, Section 0 shows the system-defined NAT rules, which are needed for the system to function properly. These show rules for internal interfaces, such as nlp_int_tap. These rules take priority over all other rules. You cannot add or change rules in Section 0.

```
ciscoasa(config)# show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source dynamic nlp_client_0_0.0.0.0_17proto53_intf3 interface
 destination static nlp_client_0_ipv4_2 nlp_client_0_ipv4_2 service nlp_client_0_17svc53_1
 nlp_client_0_17svc53_1
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.99.11.7/24
    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0
    Service - Origin: udp destination eq domain , Translated: udp destination eq domain
2 (nlp_int_tap) to (inside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.2/32, Translated: 10.99.11.7/24
3 (nlp_int_tap) to (inside) source dynamic nlp_client_0_ipv6_::_17proto53_intf3 interface
ipv6  destination static nlp_client_0_ipv6_4 nlp_client_0_ipv6_4 service
nlp_client_0_17svc53_3 nlp_client_0_17svc53_3
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: fd00:0:0:1::2/128, Translated:
    Destination - Origin: ::/0, Translated: ::/0
    Service - Origin: udp destination eq domain , Translated: udp destination eq domain
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.

show nat divert-table

To display statistics of NAT divert table, use the **show nat divert-table** command in privileged EXEC mode.

show nat divert-table [**self-addressed**] [**ipv6**] [**interface** *name*]

Syntax Description

ipv6	(Optional) Shows IPv6 entries in the divert table.
interface *name*	(Optional) Limits output to the specified source interface.
self-addressed	Show the self-addressed identity table.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.
9.18(1)	The **self-addressed** keyword was added.

Usage Guidelines

Use the **show nat divert-table** command to show runtime representation of the NAT divert table. Use the **ipv6** optional keyword to view the IPv6 entries in the divert table. Use the interface optional keyword to view the NAT divert table for the specific source interface.

Starting with 9.18(1), you might see the following information in the output:

- **do-loopback=***interface* indicates that the divert rule will trigger loopback on the specified interface.
- **rst-possible-loopback=***interface* indicates that the divert rule is for from-the-box control plane (CP) traffic and loopback might or might not occur on the specified interface.
- **nlp-possible-loopback=***interface* indicates that the divert rule is for from/to-the-box non-Lina process (NLP) traffic and loopback might or might not occur on the specified interface.

Examples

The following is sample output from the **show nat divert-table** command:

```
ciscoasa# show nat divert-table
```

```
Divert Table
id=0xad1521b8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.119.255, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1523a8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=10.86.116.0, mask=255.255.255.255, port=0-0
        input_ifc=outside, output_ifc=NP Identity Ifc
id=0xad1865c0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.255.255, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad1867b0, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=192.168.0.0, mask=255.255.255.255, port=0-0
        input_ifc=amallio-wizard, output_ifc=NP Identity Ifc
id=0xad257bf8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.255, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
id=0xad257db8, domain=twice-nat section=1 ignore=no
        type=none, hits=0, flags=0x9, protocol=0
        src ip/id=0.0.0.0, mask=0.0.0.0, port=0-0
        dst ip/id=172.27.48.0, mask=255.255.255.255, port=0-0
        input_ifc=folink, output_ifc=NP Identity Ifc
```

The following is sample output from the **show nat divert ipv6** command:

```
ciscoasa# show nat divert ipv6
Divert Table
id=0xcb9ea518, domain=divert-route
type=static, hits=0, flags=0x21, protocol=0
src ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
dst ip/id=2001::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=outside
id=0xcf24d4b8, domain=divert-route
type=static, hits=0, flags=0x20, protocol=0
src ip/id=::/::, port=0-0
dst ip/id=2222::/ffff:ffff:ffff:ffff:ffff:ffff::, port=0-0
input_ifc=in, output_ifc=mgmt
```

The following example shows the self-addressed table.

```
ciscoasa# show nat divert-table self-addressed

Self-Addressed Divert
192.168.1.33    255.255.255.255                            management to identity
1002::10        ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff    outside to identity
102.1.1.10      255.255.255.255                            outside to identity
1001::10        ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff    inside to identity
101.1.1.10      255.255.255.255                            inside to identity
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
show nat	Displays runtime representation of the NAT policies.

show nat pool

To display statistics of NAT pool usage, use the **show nat pool** command in privileged EXEC mode.

show nat pool [**interface** *if_name* [**ip** *address*] | **ip** *address*] [**detail**]
show nat pool cluster [**summary | interface** *if_name* [**ip** *address*] | **ip** *address*]

Syntax Description

cluster [**summary**]	(Optional) When ASA clustering is enabled, shows the current assignment of a PAT address to the owner unit and backup unit. (9.15+) Include the **summary** keyword to see the distribution of port blocks among the units in the cluster.
interface *if_name*	Limit the display to pools for the named interface. You can optionally include the **ip** keyword to futher limit the view.
ip *address*	Limit the display to the specified IP address from the PAT pool.
detail	Show information related to the usage and distribution of port blocks within a cluster. This keyword appears only if the unit is a cluster member. You cannot use it with the **cluster** keyword.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
8.4(3)	The output was modified to show the destination address for extended PAT. The PAT range was also modified depending on the use of the **flat** and **include-reserve** keywords.
9.0(1)	Support for IPv6 traffic and the **cluster** keyword to show the current assignment of a PAT address to the owner unit and backup unit were added.
9.15(1)	The following keywords were added: **interface** , **ip** , **detail** , **summary** .

Usage Guidelines

A NAT pool is created for each mapped protocol/IP address/port range. (Pre-9.15) The port ranges are 1-511, 512-1023, and 1024-65535 by default. If you use the **flat** keyword for a PAT pool in the **nat** command, you will see fewer, larger ranges.

(9.15+) Starting with 9.15, the port range is flat by default, and you can optionally include the reserved ports, 1-1023, in the pool. For clustered systems, the PAT pool is distributed among the cluster members in blocks of 512 ports.

Each NAT pool exists for at least 10 minutes after the last usage. The 10 minute hold-down timer is canceled if you clear the translations with **clear xlate** .

Examples

The following is sample output for the NAT pools created by a dynamic PAT rule shown by the **show running-config object network** command.

```
ciscoasa(config)# show running-config object network
object network myhost
 host 10.10.10.10
 nat (pppoe2,inside) dynamic 10.76.11.25
ciscoasa# show nat pool
TCP inside, address 10.76.11.25, range 1-511, allocated 0
TCP inside, address 10.76.11.25, range 512-1023, allocated 0
TCP inside, address 10.76.11.25, range 1024-65535, allocated 1
```

(Pre-9.15) The following is sample output from the **show nat pool** command showing use of the PAT pool **flat** option. Without the **include-reserve** keyword, two ranges are shown; the lower range is used when a source port below 1024 is mapped to the same port.

```
ciscoasa# show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-1024, allocated 0
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1024-65535, allocated 2
```

(Pre-9.15) The following is sample output from the **show nat pool** command showing use of the PAT pool **flat include-reserve** options.

```
ciscoasa# show nat pool
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 2
```

(Pre-9.15) The following is sample output from the **show nat pool** command showing use of the PAT pool **extended** **flat include-reserve** options. The important items are the parenthetical addresses. These are the destination addresses used to extend PAT.

```
ICMP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535, allocated 2
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
UDP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
ICMP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.100), range 1-65535, allocated 1
TCP PAT pool dynamic-pat, address 172.16.2.200(172.16.2.99), range 1-65535, allocated 2
UDP PAT pool dynamic-pat, address 172.16.2.200, range 1-65535, allocated 0
```

(9.15+) The following example shows the distribution of port blocks (showing the port range), and their usage, in a cluster, including the unit that owns the block and the backup unit for the block.

```
ciscoasa# show nat pool cluster

IP outside_a:src_map_a 174.0.1.20
               [1536 - 2047], owner A, backup B
               [8192 - 8703], owner A, backup B
               [4089 - 4600], owner B, backup A
               [11243 - 11754], owner B, backup A
IP outside_a:src_map_a 174.0.1.21
               [1536 - 2047], owner A, backup B
               [8192 - 8703], owner A, backup B
               [4089 - 4600], owner B, backup A
               [11243 - 11754], owner B, backup A
IP outside_b:src_map_b 174.0.1.22
               [6656 - 7167], owner A, backup B
               [13312 - 13823], owner A, backup B
               [20480 - 20991], owner B, backup A
               [58368 - 58879], owner B, backup A
IP outside_b:src_map_b 174.0.1.23
               [46592 - 47103], owner A, backup B
               [52224 - 52735], owner A, backup B
               [62976 - 63487], owner B, backup A
```

(9.15+) The following example shows a summary of pool assignments in a cluster.

```
ciscoasa# show nat pool cluster summary

port-blocks count display order: total, unit-A, unit-B, unit-C, unit-D
IP outside_a:src_map_a, 174.0.1.20 (128 - 32/32/32/32)
IP outside_a:src_map_a, 174.0.1.21 (128 - 36/32/32/28)
IP outside_b:src_map_b, 174.0.1.22 (128 - 31/32/32/33)
```

(9.16+) The following example shows a summary of pool assignments in a cluster. Starting with 9.16, the information includes the number of reserved ports and reclaimed ports.

```
ciscoasa# show nat pool cluster summary

port-blocks count display order: total, unit-A, unit-B
Codes: ^ - reserve, # - reclaimable
IP Outside:Mapped-IPGroup 10.10.10.100 (126 - 63 / 63) ^ 0 # 0
IP Outside:Mapped-IPGroup 10.10.10.101 (126 - 63 / 63) ^ 0 # 0
```

(9.15+) The following example shows detailed PAT pool usage for the pools in a cluster.

```
ciscoasa# show nat pool detail

TCP PAT pool outside_a, address 174.0.1.1
                 range 1536-2047, allocated 56
                 range 8192-8703, allocated 16
UDP PAT pool outside_a, address 174.0.1.1
                 range 1536-2047, allocated 12
                 range 8192-8703, allocated 25
 TCP PAT pool outside_b, address 174.0.2.1
                 range 47104-47615, allocated 39
                 range 62464-62975, allocated 9
UDP PAT pool outside_b, address 174.0.2.1
                 range 47104-47615, allocated 35
                 range 62464-62975, allocated 27
```

(9.15+) The following example shows how to limit the view to a specific interface on a specific device.

```
ciscoasa# show nat pool interface outside_b ip 174.0.2.1

TCP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 0
TCP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 12
TCP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 48
UDP PAT pool outside_b, address 174.0.2.1, range 1-511, allocated 6
UDP PAT pool outside_b, address 174.0.2.1, range 512-1023, allocated 8
UDP PAT pool outside_b, address 174.0.2.1, range 1024-65535, allocated 62
```

Related Commands

Command	Description
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
show nat	Displays NAT policy statistics.

show nat proxy-arp

To display the NAT proxy ARP table, use the **show nat proxy-arp** command in privileged EXEC mode.

show nat proxy-arp [**ipv6**] [**interface** *name*]

Syntax Description

ipv6	(Optional) Shows IPv6 entries in the proxy ARP table.
interface *name*	(Optional) Limits output to the specified source interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

Use the **show nat proxy-arp** command to show runtime representation of the NAT proxy ARP table. Use the **ipv6** optional keyword to view the IPv6 entries in the proxy ARP table. Use the interface optional keyword to view the NAT proxy ARP table for the specific source interface.

Examples

The following is sample output from the **show nat proxy-arp** command:

```
ciscoasa# show nat proxy-arp
Nat Proxy-arp Table
id=0x00007f5558bbbfc0, ip/id=10.10.1.134, mask=255.255.255.255 ifc=test2
 config:(inside) to (test2) source dynamic inside_v6 outside_v4_pat  destination
static inside_v6_nat any
id=0x00007f5558bbbfc0, ip/id=10.10.1.135, mask=255.255.255.255 ifc=test2
 config:(inside) to (test2) source dynamic inside_v6 outside_v4_pat  destination
static inside_v6_nat any
id=0x00007f55595ad2c0, ip/id=10.86.118.2, mask=255.255.255.255 ifc=inside
 config:(inside) to (test2) source dynamic inside_v6 interface  dns
id=0x00007f5559424e80, ip/id=10.100.10.1, mask=255.255.255.255 ifc=NP Identity Ifc
 config:(any) to (any) source dynamic src_network pat-pool mapped-pat-pool
id=0x00007f5559424e80, ip/id=10.100.10.2, mask=255.255.255.255 ifc=NP Identity Ifc
 config:(any) to (any) source dynamic src_network pat-pool mapped-pat-pool
id=0x00007f5544785700, ip/id=10.7.17.2, mask=255.255.255.254 ifc=NP Identity Ifc
```

```
 config:(any) to (any) source static test2 10.3.3.0
id=0x00007f554c4ae740, ip/id=10.1.1.1, mask=255.255.255.255 ifc=NP Identity Ifc
```

Related Commands

Command	Description
clear nat counters	Clears NAT policy counters.
nat	Identifies addresses on one interface that are translated to mapped addresses on another interface.
show nat	Displays runtime representation of the NAT policies.

show ntp associations

To view NTP association information, use the **show ntp associations** command in user EXEC mode.

show ntp associations [**detail**]

Syntax Description

detail	(Optional) Shows additional details about each association.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ntp associations** command:

```
ciscoasa> show ntp associations
     address         ref clock     st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1      5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111    3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111    3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

Table 10-2 shows each field description.

Table 75: show ntp associations Fields

Field	Description
(leading characters in display lines)	The first characters in a display line can be one or more of the following characters: • * —Synchronized to this peer. • # —Almost synchronized to this peer. • + —Peer selected for possible synchronization. • - —Peer is a candidate for selection. • ~ —Peer is statically configured, but not synchronized.
address	The address of the NTP peer.
ref clock	The address of the reference clock of the peer.
st	The stratum of the peer.
when	The time since the last NTP packet was received from the peer.
poll	The polling interval (in seconds).
reach	The peer reachability (as a bit string, in octal).
delay	The round-trip delay to the peer (in milliseconds).
offset	The relative time of the peer clock to the local clock (in milliseconds).
disp	The dispersion value.

Examples

The following is sample output from the **show ntp associations detail** command:

```
ciscoasa> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87   0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74   0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62   16000.0
```

Table 10-3 shows each field description.

Table 76: show ntp associations detail Fields

Field	Description
IP-address configured	The server (peer) IP address.
(status)	• our_master—The ASA is synchronized to this peer. • selected—Peer is selected for possible synchronization. • candidate—Peer is a candidate for selection.
(sanity)	• sane—The peer passes basic sanity checks. • insane—The peer fails basic sanity checks.
(validity)	• valid—The peer time is believed to be valid. • invalid—The peer time is believed to be invalid. • leap_add—The peer is signaling that a leap second will be added. • leap-sub—The peer is signaling that a leap second will be subtracted.
stratum	The stratum of the peer.
(reference peer)	unsynced—The peer is not synchronized to any other machine. ref ID—The address of the machine that the peer is synchronized to.
time	The last time stamp the peer received from its master.
our mode client	Our mode relative to the peer, which is always client.
peer mode server	The mode of the peer relative to the server.
our poll intvl	Our poll interval to the peer.
peer poll intvl	The peer poll interval to us.
root delay	The delay along the path to the root (ultimate stratum 1 time source).
root disp	The dispersion of the path to the root.
reach	The peer reachability (as a bit string in octal).
sync dist	The peer synchronization distance.
delay	The round-trip delay to the peer.
offset	The offset of the peer clock relative to our clock.
dispersion	The dispersion of the peer clock.
precision	The precision of the peer clock (in hertz).

Field	Description
version	The NTP version number that the peer is using.
org time	The originate time stamp.
rcv time	The receive time stamp.
xmt time	The transmit time stamp.
filtdelay	The round-trip delay (in milliseconds) of each sample.
filtoffset	The clock offset (in milliseconds) of each sample.
filterror	The approximate error of each sample.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp status	Shows the status of the NTP association.

show ntp status

To show the status of each NTP association, use the **show ntp status** command in user EXEC mode.

show ntp status

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

See the “Examples” section for a description of the display output.

Examples

The following is sample output from the **show ntp status** command:

```
ciscoasa> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

Table 10-4 shows each field description.

Table 77: show ntp status Fields

Field	Description
Clock	• synchronized—The ASA is synchronized to an NTP server. • unsynchronized—The ASA is not synchronized to an NTP server.
stratum	NTP stratum of this system.
reference	The address of the NTP server to which the ASA is synchronized.

Field	Description
nominal freq	The nominal frequency of the system hardware clock.
actual freq	The measured frequency of the system hardware clock.
precision	The precision of the clock of this system (in hertz).
reference time	The reference time stamp.
clock offset	The offset of the system clock to the synchronized peer.
root delay	The total delay along the path to the root clock.
root dispersion	The dispersion of the root path.
peer dispersion	The dispersion of the synchronized peer.

Related Commands

Command	Description
ntp authenticate	Enables NTP authentication.
ntp authentication-key	Sets an encrypted authentication key to synchronize with an NTP server.
ntp server	Identifies an NTP server.
ntp trusted-key	Provides a key ID for the ASA to use in packets for authentication with an NTP server.
show ntp associations	Shows the NTP servers with which the ASA is associated.

show nve

To show the parameters, status and statistics of an NVE interface, use the **show nve** command in privileged EXEC mode.

show nve [**1**] [**summary**]

Syntax Description

1	(Optional) Specifies the NVE instance, which is always 1.
summary	(Optional) Only shows the status of the NVE interface, number of VNIs behind the NVE interface, and number of VTEPs discovered.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	We added this command.
9.17(1)	Added output for ASA virtual cluster control link peer group. Added output for Geneve encapsulation.

Usage Guidelines

This command shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source-interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.

Examples

See the following output for the **show nve 1** command:

```
ciscoasa(config)# show nve 1
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
```

```
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

See the following output for the **show nve 1** command for an ASA virtual cluster:

```
ciscoasa(config)# show nve 1
nve 1, source-interface "vtep-ifc" is up (nve-only cluster is ON)
 IP address 10.0.0.1, subnet mask 255.255.255.0
 Encapsulation: vxlan
 Encapsulated traffic statistics:
   14310839 packets input, 2609747129 bytes
   14475972 packets output, 3145279720 bytes
   0 packets dropped
 Number of configured static peer VTEPs: 0
 Configured static peer group: cluster
    Configured static peer group VTEPs:
        IP address 10.0.0.4 MAC address 000c.295e.38ae (learned)
        IP address 10.0.0.3 MAC address 000c.2905.0050 (learned)
        IP address 10.0.0.2 MAC address 000c.2926.8a03 (learned)
 Number of discovered peer VTEPs: 3
    Discovered peer VTEPs:
        IP address 10.0.0.4
        IP address 10.0.0.3
        IP address 10.0.0.2
 Number of VNIs attached to nve 1: 1
 VNIs attached:
        vni 1: segment-id 1, mcast-group none
```

See the following output for the **show nve 1** command for an ASA virtual Geneve interface:

```
ciscoasa# show nve 1
   nve 1, source-interface "outside" is up (nve-only cluster is OFF)
            IP address 10.0.1.11, subnet mask 255.255.255.0
            Encapsulation: geneve
            Encapsulated traffic statistics:
               1107 packets input, 84557 bytes
               83 packets output, 39784 bytes
               0 packets dropped
            Number of configured static peer VTEPs: 0
            Configured static peer group: N/A
            Number of discovered peer VTEPs: 0
            Number of VNIs attached to nve 1: 1
            VNIs attached:
               vni 1: segment-id none, aws-proxy on, mcast-group none
            NVE aws-proxy channel is on.
```

See the following output for the **show nve 1 summary** command:

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

show object

To display information about network-service objects, including hit counts and IP addresses, use the **show object** command in privileged EXEC mode..

show object [**id** *object_name* | **network-service** [**detail**]]

Syntax Description

id *name*	(Optional) The name of the object you want to view. Capitalization matters. For example "object-name" does not match "Object-Name."
network-service [**detail**]	(Optional.) Show all network-service objects. Include the detail keyword to see the cached IP addresses associated with the object members.

Command Default

Without parameters, all objects are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was introduced.

Example

The following example shows the object named partner-web. The hitcnt (hit count) number shows how often connections matched the object.

```
FP2130-2# show object id partner-web
object network-service "partner-web"
 subnet 10.100.10.0 255.255.255.0 tcp eq https (hitcnt=0)
```

Related Commands

Command	Description
clear object	Clears the object hit count.

show object-group

To display object group information and the relevant hit count if the object group is of the network or network-service object-group type, use the **show object-group** command in privileged EXEC mode.

show object-group [**count** | **network** | **protocol** | **security** | **service** | **icmp-type** | **id** *object_group_name*]

show object-group network-service [*group_name* [**network-service-member** *member_name* [**dns** *domain_name*]] [**detail**]

Syntax Description

count	(Optional.) Show statistics related to the number of object groups and the number of objects in those groups, and how they are used.
detail	For network-service objects, show the cached IP addresses associated with the object members.
dns *domain_name*	(Optional.) For network-service objects specified by name and member, limit the information to a specific domain for that member. For example, example.com.
icmp-type	(Optional) An ICMP-type object group.
id *object_group_name*	(Optional) Identifies an object group by name.
network	(Optional) Network-type objects.
network-service [*group_name*]	(Optional.) Network-service objects. You can specify the object name to limit the information to a single object.
network-service-member *member_name*	(Optional.) For network-service objects specified by name, limit the information to a specific member of that object.
protocol	(Optional) Protocol-type object group.
security	(Optional) Security-type objects
service	(Optional) Service-type object.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.17(1)	We added the **network-service** keyword and its associated parameters.
9.18(1)	The **count** keyword was added.

Examples

The following is sample output from the **show object-group** command and shows information about the network object group named “Anet”:

```
ciscoasa# show object-group id Anet
Object-group network Anet (hitcnt=10)
   Description OBJ SEARCH ALG APPLIED
   network-object 1.1.1.0 255.255.255.0 (hitcnt=4)
   network-object 2.2.2.0 255.255.255.0 (hitcnt=6)
```

The following is sample output from the **show object-group** command and shows information about a service group:

```
ciscoasa (config)# show object-group service
object-group service B-Serobj
   description its a service group
   service-object tcp eq bgp
   object-group protocol C-grp-proto
   protocol-object ospf
```

The following is sample output from the **show object-group** command and shows information about a protocol:

```
ciscoasa (config)# show object-group protocol
object-group protocol C-grp-proto
   protocol-object ospf
```

The following example shows a network-service object and its hit counts. The various identifiers, such as network-service group ID (nsg-id), application ID (app-id), and bid are internal indexing numbers that you can ignore.

```
ciscoasa (config)# show object-group network-service FMC_NSG_4294969442
object-group network-service FMC_NSG_4294969442 (nsg-id 512/1)
 network-service-member "Facebook" dynamic
  description Facebook is a social networking service.
  app-id 629
  domain connect.facebook.net (bid=214491) ip (hitcnt=0)
  domain facebook.com (bid=370809) ip (hitcnt=0)
  domain fbcdn.net (bid=490321) ip (hitcnt=0)
  domain fbcdn-photos-a.akamaihd.net (bid=548791) ip (hitcnt=0)
  domain fbcdn-photos-e-a.akamaihd.net (bid=681143) ip (hitcnt=0)
  domain fbcdn-photos-b-a.akamaihd.net (bid=840741) ip (hitcnt=0)
  domain fbstatic-a.akamaihd.net (bid=1014669) ip (hitcnt=0)
  domain fbexternal-a.akamaihd.net (bid=1098051) ip (hitcnt=0)
  domain fbcdn-profile-a.akamaihd.net (bid=1217875) ip (hitcnt=0)
  domain fbcdn-creative-a.akamaihd.net (bid=1379985) ip (hitcnt=0)
  domain channel.facebook.com (bid=1524617) ip (hitcnt=0)
  domain fbcdn-dragon-a.akamaihd.net (bid=1683343) ip (hitcnt=0)
  domain contentcache-a.akamaihd.net (bid=1782703) ip (hitcnt=0)
  domain facebook.net (bid=1868733) ip (hitcnt=0)
 network-service-member "Google+ Videos" dynamic
  description Video sharing among Google+ community.
  app-id 2881
  domain plus.google.com (bid=2068293) ip (hitcnt=0)
 network-service-member "Instagram" dynamic
  description Mobile phone photo sharing.
  app-id 1233
  domain instagram.com (bid=2176667) ip (hitcnt=0)
 network-service-member "LinkedIn" dynamic
  description Career oriented social networking.
  app-id 713
  domain linkedin.com (bid=2317259) ip (hitcnt=0)
>
```

The following example shows object counts, so you have an idea of how many object groups there are, how many objects are contained in the groups, and how many are used in ACLs, NAT, and so forth. This information relates to the performance of the object group search feature.

```
ciscoasa(config)# show object-group count

Object Group Name                       Group Count Dyn Count V4 CNT     V6 CNT     ACL CNT
    NAT CNT    OG in OG
network    i28Z-route                   68          0           68         0          0
      0          0
network    i28Z-VRF-BGP-PEERS           4           0           4          0          2
      0          0
network    EXCH-BGP-PEERS               4           0           4          0          2
      0          0
network    obgr_SUBNETS_NO_ACL          112         0           112        0          0
      0          0
network    obgr_SUBNETS_ACL_ASAMgmt     1           0           1          0          0
      0          0
network    obgr_CLIENTS_ACL_ASAMgmt     8           0           8          0          1
      0          0
network    obgr_SUBNETS_CGS_vMotion     1           0           1          0          0
      0          0
network    obgr_CLIENTS_CGS_vMotion     9           0           9          0          1
      0          0
network    obgr_SUBNETS_UPMCOD_CGS      17          0           17         0          0
      0          0
network    obgr_CLIENTS_UPMCOD_CGS      90          0           90         0          1
      0          0
network    obgr_CLIENTS_10.68.0.0_16    2           0           2          0          1
      0          0
network    obgr_CLIENTS_10.68.1.198_31 4            0           4          0          1
      0          0
network    obgr_CLIENTS_10.68.73.133    7           0           7          0          1
      0          0
network    asa_zabbix_proxies           4           0           4          0          1
      0          0

Total Summary
```

```
Object-group count                          14
Object-group object count                   331
Object-group Dynamic count                  0
Object-group IPv4 count                     331
Object-group IPv6 count                     0
Object-group Used in ACL                    9
Object-group Used in NAT                    0
Object-group Unused                         5
Object-group Internal                       0
Object-group Dummy                          0
Redundant object-group in Network           4
Redundant object-group in IfC               0
```

Related Commands

Command	Description
clear object-group	Clears the object group hit count.
show access list	Shows all access lists, relevant expanded access list entries, and hit counts.
show object	Shows network-service objects and hit counts.

show ospf

To display the general information about the OSPF routing processes, use the **show ospf** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.

Command Default

Lists all OSPF processes if no *pid* is specified.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

If the *pid* is included, only information for the specified routing process is included.

Examples

The following is sample output from the **show ospf** command, showing how to display general information about a specific OSPF routing process:

```
ciscoasa# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

The following is sample output from the **show ospf** command, showing how to display general information about all OSPF routing processes:

```
ciscoasa# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf border-routers

To display the internal OSPF routing table entries to ABRs and ASBRs, use the **show ospf border-routers** command in privileged EXEC mode.

show ospf border-routers

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output from the show **ospf border-routers** command:

```
ciscoasa# show ospf border-routers
OSPF Process 109 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf database

To display the information contained in the OSPF topological database on the ASA, use the **show ospf database** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **database** [**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external**] [*lsid*] [**internal**] [**self-originate** | **adv-router** *addr*]
show ospf [*pid* [*area_id*]] **database database-summary**

Syntax Description

addr	(Optional) Router address.
adv-router	(Optional) Advertised router.
area_id	(Optional) ID of the area that is associated with the OSPF address range.
asbr-summary	(Optional) Displays an ASBR list summary.
database	Displays the database information.
database-summary	(Optional) Displays the complete database summary list.
external	(Optional) Displays routes external to a specified autonomous system.
internal	(Optional) Routes that are internal to a specified autonomous system.
lsid	(Optional) LSA ID.
network	(Optional) Displays the OSPF database information about the network.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
pid	(Optional) ID of the OSPF process.
router	(Optional) Displays the router.
self-originate	(Optional) Displays the information for the specified autonomous system.
summary	(Optional) Displays a summary of the list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the ASA. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf database** command:

```
ciscoasa# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)
                 Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3
                 Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC
                 Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

The following is sample output from the **show ospf database asbr-summary** command:

```
ciscoasa# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database router** command:

```
ciscoasa# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
```

```
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

The following is sample output from the **show ospf database network** command:

```
ciscoasa# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

The following is sample output from the **show ospf database summary** command:

```
ciscoasa# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

The following is sample output from the **show ospf database external** command:

```
ciscoasa# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)
                   Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0
      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
```

```
Forward Address: 0.0.0.0
External Route Tag: 0
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf events

To display OSPF internal event information, use the **show ospf events** command in user EXEC or privileged EXEC mode.

show ospf [*process_id*] **events** [*type*]

Syntax Description

process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.
type	(Optional) A list of the event types you want to see. If you do not specify one or more types, you see all events. You can filter on the following types: • **generic**—Generic events. • **interface**—Interface state change events. • **lsa**—LSA arrival and LSA generation events. • **neighbor**—Neighbor state change events. • **reverse**—Show events in reverse order. • **rib**—Router Information Base update, delete and redistribution events. • **spf**—SPF scheduling and SPF run events.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—
User EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output from the **show ospf events** command:

```
ciscoasa# show ospf events
            OSPF Router with ID (192.168.77.1) (Process ID 5)
   1 Apr 27 16:33:23.556: RIB Redist, dest 0.0.0.0, mask 0.0.0.0, Up
   2 Apr 27 16:33:23.556: Rescanning RIB:  0x00x0
   3 Apr 27 16:33:23.556: Service Redist scan:  0x00x0
```

Related Commands

Command	Description
show ospf	Shows all settings in the OSPF routing process.
show ospf border-routers	Shows the internal OSPF routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ospf flood-list

To display a list of OSPF LSAs waiting to be flooded over an interface, use the **show ospf flood-list** command in privileged EXEC mode.

show ospf flood-list *interface_name*

Syntax Description

interface_name	The name of the interface for which to display neighbor information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the ASA. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

Examples

The following is sample output from the **show ospf flood-list** command:

```
ciscoasa# show ospf flood-list outside
  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID         ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0    192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0    192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0    192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0    192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0    192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0    192.168.0.163    0x80000009   0     0x134C
```

Related Commands

Command	Description
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf interface

To display the OSPF-related interface information, use the **show ospf interface** command in privileged EXEC mode.

show ospf interface [*interface_name*]

Syntax Description

interface_name	(Optional) Name of the interface for which to display the OSPF-related information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When used without the *interface_name* argument, the OSPF information for all interfaces is shown.

Examples

The following is sample output from the **show ospf interface** command:

```
ciscoasa# show ospf interface outside
out is up, line protocol is up
  Internet Address 10.0.3.4 mask 255.255.255.0, Area 0
  Process ID 2, Router ID 10.0.3.4, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State WAITING, Priority 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10 msec, Dead 1, Wait 1, Retransmit 5
    Hello due in 5 msec
    Wait time before Designated router selection 0:00:11
  Index 1/1, flood queue length 0
  Next 0x00000000(0)/0x00000000(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

show ospf neighbor

To display the OSPF-neighbor information on a per-interface basis, use the **show ospf neighbor** command in privileged EXEC mode.

show ospf neighbor [**detail** | *interface_name* [*nbr_router_id*]]

Syntax Description

detail	(Optional) Lists detail information for the specified router.
interface_name	(Optional) Name of the interface for which to display neighbor information.
nbr_router_id	(Optional) Router ID of the neighbor router.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output from the **show ospf neighbor** command. It shows how to display the OSPF-neighbor information on a per-interface basis.

```
ciscoasa# show ospf neighbor outside
Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

The following is sample output from the **show ospf neighbor detail** command. It shows how to display the detailed information for the specified OSPF-neighbor.

```
ciscoasa# show ospf neighbor detail
Neighbor 25.1.1.60, interface address 15.1.1.60
    In the area 0 via interface inside
    Neighbor priority is 1, State is FULL, 46 state changes
    DR is 15.1.1.62 BDR is 15.1.1.60
    Options is 0x12 in Hello (E-bit, L-bit)
    Options is 0x52 in DBD (E-bit, L-bit, O-bit)
    LLS Options is 0x1 (LR), last OOB-Resync 00:03:07 ago
    Dead timer due in 0:00:24
    Neighbor is up for 01:42:15
    Index 5/5, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

Related Commands

Command	Description
neighbor	Configures OSPF routers interconnecting to non-broadcast networks.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf nsf

To display the OSPFv2 related NSF information, use the **show ospf nsf** command in privileged EXEC mode.

show ospf nsf

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(1)	This command was added.

Examples

The following is sample output from the **show ospf nsf** command:

```
ciscoasa# show ospf nsf
Routing Process "ospf 10"
Non-Stop Forwarding enabled
 Clustering is not configured in spanned etherchannel mode
IETF NSF helper support enabled
Cisco NSF helper support enabled
 OSPF restart state is
 Handle 1, Router ID 25.1.1.60, checkpoint Router ID 0.0.0.0
 Config wait timer interval 10, timer not running
 Dbase wait timer interval 120, timer not running
```

Related Commands

Command	Description
nsf cisco	Enables Cisco NSF on NSF-capable router.
router ospf	Enables OSPF routing and configures global OSPF routing parameters.

show ospf request-list

To display a list of all LSAs that are requested by a router, use the **show ospf request-list** command in privileged EXEC mode.

show ospf request-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.
nbr_router_id	Router ID of the neighbor router. Displays the list of all LSAs that are requested by the router from this neighbor.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output from the **show ospf request-list** command:

```
ciscoasa# show ospf request-list 192.168.1.12 inside
          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12
  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

Related Commands

Command	Description
show ospf retransmission-list	Displays a list of all LSAs waiting to be resent.

show ospf retransmission-list

To display a list of all LSAs waiting to be resent, use the **show ospf retransmission-list** command in privileged EXEC mode.

show ospf retransmission-list *nbr_router_id interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information.
nbr_router_id	Router ID of the neighbor router.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the ASA. You do not need to be in an OSPF configuration mode to use the OSPF-related **show** commands.

The *nbr_router_id* argument displays the list of all LSAs that are waiting to be resent for this neighbor.

The *interface_name* argument displays the list of all LSAs that are waiting to be resent for this interface.

Examples

The following is sample output from the **show ospf retransmission-list** command, where the *nbr_router_id* argument is 192.168.1.11 and the *if_name* argument is outside:

```
ciscoasa# show ospf retransmission-list 192.168.1.11 outside
          OSPF Router with ID (192.168.1.12) (Process ID 1)
  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

Related Commands

Command	Description
show ospf request-list	Displays a list of all LSAs that are requested by a router.

show ospf rib

To display the OSPF Router Information Base (RIB), use the **show ospf rib** command in privileged EXEC mode.

show ospf [*pid* [*area_id*]] **rib** [*network_prefix* [*network_mask*] **| detail | redistribution** [*network_prefix* [*network_mask*] **| detail**]]

Syntax Description

area_id	(Optional) ID of the area that is associated with the OSPF address range.
pid	(Optional) The ID of the OSPF process.
network_prefix [*network_mask*]	(Optional) The network prefix and optionally the mask of the route you want to view, for example: 10.100.10.1 10.100.10.0 255.255.255.0
detail	(Optional) Display detailed information about the RIB.
redistribution	(Optional) Display redistribution information. You can also specify the network prefix and mask or **detail** keyword after the redistribution keyword.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

show ospf statistics

To display various OSPF statistics, use the **show ospf statistics** command in user EXEC or privileged EXEC mode.

show ospf [*process_id*] **statistics** [**detail**]

Syntax Description

detail	(Optional) Specifies detailed SPF information, including the trigger points.
process_id	(Optional) Specifies an internal ID that is locally assigned and can be any positive integer. This ID is the number assigned administratively when the OSPF routing process is enabled.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—
User EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use this command to list the number of times SPF was executed, the reasons, and the duration.

Examples

The following is sample output from the **show ospf statistics** command:

```
ciscoasa# show ospf 10 statistics detail
Area 10: SPF algorithm executed 6 times
SPF 1 executed 04:36:56 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
              0             0
  LSIDs processed R:1 N:0 Prefix:0 SN:0 SA:0 X7:0
  Change record R L
  LSAs changed 2
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  49.100.168.192/0(R) 49.100.168.192/2(L)
SPF 2 executed 04:35:50 ago, SPF type Full
  SPF calculation time (in msec):
  SPT    Prefix D-Int  Sum    D-Sum  Ext    D-Ext  Total
       0      0      0      0      0      0      0 0
  RIB manipulation time (in msec):
  RIB Update    RIB Delete
               0             0
  LSIDs processed R:2 N:1 Prefix:0 SN:0 SA:0 X7:0
  Change record R N L
  LSAs changed 5
  Changed LSAs. Recorded is Advertising Router, LSID and LS type:
  50.100.168.192/0(R) 50.100.168.192/2(L) 49.100.168.192/0(R) 50.100.168.192/0(R)
  50.100.168.192/2(N)
```

Related Commands

Command	Description
show ospf	Shows all settings in the OSPF routing process.
show ospf border-routers	Shows the internal OSPF routing table entries to an area border router (ABR) and an autonomous system boundary router (ASBR).

show ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the **show ospf summary-address** command in privileged EXEC mode.

show ospf summary-address

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	MSupport for multiple context mode was added.

Examples

The following shows sample output from the **show ospf summary-address** command. It shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5.

```
ciscoasa# show ospf 5 summary-address
OSPF Process 2, Summary-address
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

Related Commands

Command	Description
summary-address	Creates aggregate addresses for OSPF.

show ospf traffic

To display a list of different types of packets that have been processed (sent or received) by a particular OSPF instance, use the **show ospf traffic** command in privileged EXEC mode. With this command, you can get a snapshot of the different types of OSPF packets that are being processed without enabling debugging. If there are two OSPF instances configured, the show ospf traffic command displays the statistics for both instances with the process ID of each instance. You can also display the statistics for a single instance by using the show **ospf** *process_id* **traffic** command.

show ospf traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

With this command, you can get a snapshot of the different types of OSPF packets that are being processed without enabling debugging. If there are two OSPF instances configured, the **show ospf traffic** command displays the statistics for both instances with the process ID of each instance. You can also display the statistics for a single instance by using the **show ospf** *process_id* **traffic** command.

Examples

The following shows sample output from the **show ospf traffic** command.

```
ciscoasa# show ospf traffic
OSPF statistics (Process ID 70):
       Rcvd: 244 total, 0 checksum errors
             234 hello, 4 database desc, 1 link state req
             3 link state updates, 2 link state acks
       Sent: 485 total
             472 hello, 7 database desc, 1 link state req
             3 link state updates, 2 link state acks
```

Related Commands

Command	Description
show ospf virtual-links	Displays the parameters and the current state of OSPF virtual links.

show ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the **show ospf virtual-links** command in privileged EXEC mode.

show ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output from the **show ospf virtual-links** command:

```
ciscoasa# show ospf virtual-links
Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

Related Commands

Command	Description
area virtual-link	Defines an OSPF virtual link.

show p – show r

show packet tracer

To display information about the pcap trace output, use the **show packet tracer** command.

show packet-tracer pcap trace [**packet-number** *number* | **summary** | **detailed** | **status**]

Syntax Description

packet-number	(Optional) Displays trace output for a single packet in pcap.
summary	(Optional) Displays pcap summary.
detailed	(Optional) Displays trace output for all packets in pcap.
status	(Optional) Displays the current execution state of pcap trace.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.17.1	The command was enhanced to include output of pcap trace.

Usage Guidelines

The **show packet-tracer** command shows the packet tracer output. The **pcap trace** command allows you to display the trace buffer output of the most recently run packet-tracer on a PCAP file.

Examples

The following is sample output for the **show packet-tracer pcap trace summary** command:

```
ciscoasa# show packet-tracer pcap trace summary
     1: 02:38:01.265123       6.1.1.100.51944 > 9.1.1.100.80: S 542888804:542888804(0) win
 29200 <mss 1460,sackOK,timestamp 2526545680 0,nop,wscale 7>
      2: 02:38:01.271317       9.1.1.100.80 > 6.1.1.100.51944: S 2281169942:2281169942(0)
ack 542888805 win 28960 <mss 1380,sackOK,timestamp 2526520070 2526545680,nop,wscale 7>
      3: 02:38:01.271638       6.1.1.100.51944 > 9.1.1.100.80: . ack 2281169943 win 229
<nop,nop,timestamp 2526545682 2526520070>

                Total packets: 3
       Packets replayed: 3
       Result: Allow
       Start time: Mar 28 04:51:54
       Total time taken: 10247935ns
     show packet-tracer pcap trace packet-number 1 detailed
     1: 02:38:01.265123 0050.56a9.81e5 0050.56a9.60e1 0x0800 Length: 74
      6.1.1.100.51944 > 9.1.1.100.80: S [tcp sum ok] 542888804:542888804(0) win 29200 <mss
 1460,sackOK,timestamp 2526545680 0,nop,wscale 7> (DF) (ttl 64, id 54388)
      Phase: 1
      Type: ACCESS-LIST
      Subtype:
      Result: ALLOW
      Time Spent: 12345 ns
      Config:
      Implicit Rule
      Additional Information:
      Forward Flow based lookup yields rule:
       in  id=0x154523db3ce0, priority=1, domain=permit, deny=false
                       hits=92, user_data=0x0, cs_id=0x0, l3_type=0x8
                       src mac=0000.0000.0000, mask=0000.0000.0000
                       dst mac=0000.0000.0000, mask=0100.0000.0000
                       input_ifc=inside, output_ifc=any
       …
       …
```

Related Commands

Command	Description
packet tracer	Generates a 5-to-6 tuple packet against a firewall’s current configurations

show packet-statistics

To display information about any packet drops on the Secure Firewall 3100, use the **show packet-statistics** command.

show packet-statistics *interface_id* [**brief**]

Syntax Description

interface_id	Interface ID for which the statistics are displayed.
brief	(Optional) Displays the output excluding the zero counter values.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.18(1)	This command was introduced.

Usage Guidelines

The **show packet-statistics** command collates and displays packet loss data from several sources in the operating system. The output helps to identify where the packets were dropped. This command consolidates the output of the following commands:

- FXOS:
  - **show portmanager counters ethernet**
  - **show queuing interface ethernet**
  - **show portmanager counters internal**
  - **show queuing interface internal**
  - **show portmanager switch counters packet-trace**
  - FPGA: **show npu-accel statistics**
  - ASA:
    - **show interface detail**
    - **show asp drop**

The consolidated output is in the sequence of the data path when traffic reach a device. In addition, the output is not broken or interrupted by other CLIs' output.

Examples

The following is sample output for the **show packet-statistics** command:

```
ciscoasa# show packet-statistics Ethernet 1/1
============= show portmanager counters Ethernet 1 1 ==============
Good Octets Received : 66882
Bad Octets Received : 0
MAC Transmit Error : 0
…
…
============= show queuing interface Ethernet 1 1 ==============
Queue Traffic-type Scheduler-type oper-bandwidth Destination
----------------------------------------------------------------------------
3 Data WRR 100 Application
4 CCL-CLU SP 0 Application
5 BFD SP 0 Application
…
…
…
============= show portmanager counters Internal 1 1 ==============
Good Octets Received : 3770
Bad Octets Received : 0
MAC Transmit Error : 0
…
…
============= show queuing interface Internal 1 1 ==============
Queue Traffic-type Scheduler-type oper-bandwidth Destination
----------------------------------------------------------------------------
3 Data WRR 100 Application
4 CCL-CLU SP 0 Application
5 BFD SP 0 Application
…
…
====================== show portmanager switch counters packet-trace ======================
Counter Source port- 0/0 Destination port- 0/0
----------------------- --------------------- ---------------------
goodOctetsRcv --- ---
badOctetsRcv --- ---
Ingress counters
gtBrgInFrames 5 5
gtBrgVlanIngFilterDisc 0 0
…
…
====================== show npu-accel statistics ======================
module: kc50-pcie, pipe: 0
--------------------------
reg_pcie_rcv_reg_access_rd_tlp_cnt = 1312987327
reg_pcie_rcv_reg_access_wr_tlp_cnt = 227526828
…
…
====================== show interface detail ======================
Interface Ethernet1/1 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Auto-Duplex, Auto-Speed
Available but not configured via nameif
MAC address f87a.410e.5994, MTU not set
…
…
```

```
======================= show asp drop ======================
Frame drop:
Slowpath security checks failed (sp-security-failed) 18
FP L2 rule drop (l2_acl) 118
Interface is down (interface-down) 11
Last clearing: Never
```

show pager

To display a default or static route for an interface, use the **show pager** command in privileged EXEC mode.

show pager

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
4.0(1)	This command was added.

Examples

The following is sample output from the **show pager** command:

```
ciscoasa(config)# show pager
pager lines 0
```

Related Commands

Command	Description
clear configure pager	Removes the number of lines set to display in a Telnet session before the “---More---” prompt appears from the running configuration.
show running-config pager	Displays the number of lines set to display in a Telnet session before the “---More---” prompt appears in the running configuration.
terminal pager	Sets the number of lines to display in a Telnet session before the “---More---” prompt appears. This command is not saved to the running configuration.

show path-monitoring

To display information about the path monitoring output, use the **show path monitoring** command.

show path-monitoring [**interface** *name*] [**detail**]

Syntax Description

Interface*name*	Interface for which the path monitoring metric is displayed
detail	(Optional) Displays detailed information about path monitoring metrics.

Command Default

No default behavior or values.

Command History

Release	Modification
9.18(1)	The command was introduced to display the path monitoring details for a specified interface.

Usage Guidelines

The **show path-monitoring** command shows the path monitoring output for the specified egress interface.

Examples

The following is sample output for the **show path-monitoring** command for *outside 1* interface:

```
ciscoasa# show path-monitoring interface outside1
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 1 second(s) ago
```

The following is sample output for the **show path-monitoring detail** command for *outside 1* interface:

```
ciscoasa#
firepower# show path-monitoring interface outside1 detail
Interface: outside1
Remote peer: 90.2.1.1
    Version: 14275
    Remote peer reachable: Yes
    RTT average: 1407 microsecond(s)
    Jitter: 1218 microsecond(s)
    Packet loss: 0%
    MOS: 4.40
    Last updated: 8 second(s) ago

    Internal data:
        Total probes sent: 418553
        Total probes pending: 0
        Current probes pending: 0
        Current RTT sum: 51674
        Current RTT square sum: 154410282
```

```
Flags: 0x2
Current queue index: 14
Index:  0, Timestamp:              0, RTT:     962
Index:  1, Timestamp:              0, RTT:    1096
Index:  2, Timestamp:              0, RTT:    1056
Index:  3, Timestamp:              0, RTT:    1457
Index:  4, Timestamp:              0, RTT:    1078
Index:  5, Timestamp:              0, RTT:    1114
Index:  6, Timestamp:              0, RTT:    1570
Index:  7, Timestamp:              0, RTT:    6865
Index:  8, Timestamp:              0, RTT:    1035
Index:  9, Timestamp:              0, RTT:    1334
Index: 10, Timestamp:              0, RTT:    1090
Index: 11, Timestamp:              0, RTT:    1099
Index: 12, Timestamp:              0, RTT:    1429
Index: 13, Timestamp:              0, RTT:    1048
Index: 14, Timestamp:              0, RTT:     985
Index: 15, Timestamp:              0, RTT:    1002
Index: 16, Timestamp:              0, RTT:    1013
Index: 17, Timestamp:              0, RTT:    1741
Index: 18, Timestamp:              0, RTT:    1231
Index: 19, Timestamp:              0, RTT:    1517
Index: 20, Timestamp:              0, RTT:    7780
Index: 21, Timestamp:              0, RTT:    1018
Index: 22, Timestamp:              0, RTT:    1036
Index: 23, Timestamp:              0, RTT:    2369
Index: 24, Timestamp:              0, RTT:    1120
Index: 25, Timestamp:              0, RTT:    1062
Index: 26, Timestamp:              0, RTT:    1088
Index: 27, Timestamp:              0, RTT:    1073
Index: 28, Timestamp:              0, RTT:    1060
Index: 29, Timestamp:              0, RTT:    1071
Index: 30, Timestamp:              0, RTT:    1116
Index: 31, Timestamp:              0, RTT:    1075
Index: 32, Timestamp:              0, RTT:    1084
```

Related Commands

Command	Description
policy-route	Configures policy based routing on an interface.

show password encryption

To show the password encryption configuration settings, use the **show password encryption** command in privileged EXEC mode.

show password encryption

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.3(1)	This command was added.
8.4(1)	Show password encryption in user context was added.

Usage Guidelines

If the key has been saved using the **write memory** command, “saved” appears next to the key hash. If there is no key or it has been removed from the running configuration, “Not set” appears instead of the hash value.

Examples

The following is sample output from the **show password encryption** command:

```
ciscoasa# show password encryption
Password Encryption: Enabled
Master key hash: 0x35859e5e 0xc607399b 0x35a3438f 0x55474935 0xbec1ee7d(not saved)
```

Related Commands

Command	Description
password encryption aes	Enables password encryption.
key config-key password-encrypt	Sets the pass phrase used for generating the encryption key.

show perfmon

To display information about the performance of the ASA, use the **show perfmon** command in privileged EXEC mode.

show perfmon [**detail**]

Syntax Description

detail	(Optional) Shows additional statsistics. These statistics match those gathered by the Global and Per-protocol connection objects of the Cisco Unified Firewall MIB.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	Support for this command was added on the ASA.
7.2(1)	The **detail** keyword was added.

Usage Guidelines

This command output does not display in a Telnet session.

The perfmon command shows performance statistics continuously at defined intervals. The show perfmon command allows you to display the information immediately.

Note ASA takes time to calculate and display the Current and Average counters with accurate values. The default value for the Perfmon Stat Refresh interval for the Current value is 120 seconds. The Average counter is calculated based on the average of the values from the last time **clear perfmon** was executed or when the command was not used, from the time the device was started.

Examples

The following is sample output for the **show perfmon** command:

```
ciscoasa(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
```

```
UDP Conns           0/s          0/s
URL Access          0/s          0/s
URL Server Req      0/s          0/s
WebSns Req          0/s          0/s
TCP Fixup           0/s          0/s
TCP Intercept       0/s          0/s
HTTP Fixup          0/s          0/s
FTP Fixup           0/s          0/s
AAA Authen          0/s          0/s
AAA Author          0/s          0/s
AAA Account         0/s          0/s
```

The following is sample output for the **show perfmon detail** command:

```
ciscoasa(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates              0/s          0/s
Connections         0/s          0/s
TCP Conns           0/s          0/s
UDP Conns           0/s          0/s
URL Access          0/s          0/s
URL Server Req      0/s          0/s
TCP Fixup           0/s          0/s
HTTP Fixup          0/s          0/s
FTP Fixup           0/s          0/s
AAA Authen          0/s          0/s
AAA Author          0/s          0/s
AAA Account         0/s          0/s
TCP Intercept       0/s          0/s
SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

Related Commands

Command	Description
perfmon	Displays detailed performance monitoring information at defined intervals.

show phone-proxy (Deprecated)

To show phone-proxy specific information, use the **show phone-proxy** command in global configuration mode.

show phone-proxy [**media-sessions** [**detail**] | **signaling-sessions** [**detai**] | **secure-phones**]

Syntax Description

detail	Displays detailed information.
media-sessions	Displays the corresponding media sessions stored by the Phone Proxy. In addition, displays the media-termination address configured for the interface between which the media sessions are established.
secure-phones	Displays the phones capable of secure mode stored in the database.
signaling-sessions	Displays the corresponding signaling sessions stored by the Phone Proxy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
8.2(1)	The command was updated so that specifying the **media-sessions** keyword also displays the media-termination address configured for the interface between which the media sessions are established.
9.4(1)	This command was deprecated along with all **phone-proxy** mode commands.

Examples

The following example shows the use of the **show phone proxy** command to show Phone Proxy specific information:

```
ciscoasa
(config)#
show phone-proxy
Phone-Proxy 'mypp': Runtime Proxy ref_cnt 2
Cluster Mode: nonsecure
Run-time proxies:
Proxy 0xd55f6fd8: Class-map: secsip, Inspect: sip
Proxy 0xd58a93a8: Class-map: secsccp, Inspect: skinny
phoneproxy(config)# show phone-proxy secure-phones
mypp: 5 in use, 5 most used
Interface  IP Address      Port  MAC            Timeout Idle
outside    69.181.112.219 10889 001e.7ac4.da9c 0:05:00 0:01:36
outside    98.208.25.87   14159 001c.581c.0663 0:05:00 0:00:04
outside    98.208.25.87   14158 0007.0e36.4804 0:05:00 0:00:13
outside    98.208.25.87   14157 001e.7ac4.deb8 0:05:00 0:00:21
outside    128.107.254.69 49875 001b.0cad.1f69 0:05:00 0:00:04
ciscoasa
(config)#
```

The following example shows the use of the **show phone proxy** command to display the phones capable of secure mode stored in the database:

```
ciscoasa
(config)#
 show phone-proxy secure-phones
asa_phone_proxy: 3 in use, 4 most used
Interface/IP Address      MAC              Timeout    Idle
------------------------  ----------       ---------  ------
outside:69.181.112.219    001e.7ac4.da9c    0:05:00    0:00:16
outside:69.181.112.219    0002.b9eb.0aad    0:05:00    0:00:58
outside:98.208.49.30      0007.0e36.4804    0:05:00    0:00:09
ciscoasa
(config)#
```

The following example shows the use of the **show phone proxy** command to show output from a successful call and the media-termination address configured for the interface between which the media sessions are established:

```
ciscoasa
(config)#
 show phone-proxy media-sessions

Media-session: 128.106.254.3/1168 refcnt 6
  <---> RTP connection to 192.168.200.106/25038 tx_pkts 485 rx_pkts 491
Media-session: 128.106.254.3/1170 refcnt 6
  <---> SRTP connection to 98.208.25.87/1030 tx_pkts 484 rx_pkts 485
```

Related Commands

Command	Description
debug phone-proxy	Displays debug messages for the Phone Proxy instance.
phone proxy	Configures the Phone Proxy instance.

show pim bsr-router

To display the bootstrap router (BSR) information, use the show pim bsr-router command

show pim bsr-router

Syntax Description

No arguments or variables.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.

Examples

The following is sample output from the **show pim bsr-router** command:

```
ciscoasa# show pim bsr-router
PIMv2 Bootstrap information
This system is a candidate BSR
  Candidate BSR interface GigabitEthernet0/0 is down - BSR messages not originated
  Candidate RP: 4.4.4.1(GigabitEthernet0/0), GigabitEthernet0/0 is down - not advertised
```

show pim df

To display the bidirectional DF "winner" for a rendezvous point (RP) or interface, use the **show pim df** command in user EXEC or privileged EXEC mode.

show pim df [**winner**] [*rp_address* | *if_name*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.
if_name	The physical or logical interface name.
winner	(Optional) Displays the DF election winner per interface per RP.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command also displays the winner metric towards the RP.

Examples

The following is sample output from the **show pim df** command:

```
ciscoasa# show pim df
RP            Interface    DF Winner    Metrics
172.16.1.3    Loopback3    172.17.3.2   [110/2]
172.16.1.3    Loopback2    172.17.2.2   [110/2]
172.16.1.3    Loopback1    172.17.1.2   [110/2]
172.16.1.3    inside       10.10.2.3    [0/0]
172.16.1.3    inside       10.10.1.2    [110/2]
```

show pim group-map

To display group-to-protocol mapping table, use the **show pim group-map** command in privileged EXEC mode.

show pim group-map [**info-source**] [*group*]

Syntax Description

group	(Optional) Can be either one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
info-source	(Optional) Displays the group range information source.
rp-timers	(Optional) Displays uptime and expiry timers of group-to-RP mapping.

Command Default

Displays group-to-protocol mappings for all groups.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was modified to include the rp-timers variable.

Usage Guidelines

This command displays all group protocol address mappings for the RP. Mappings are learned on the ASA from different clients.

The PIM implementation on the ASA has various special entries in the mapping table. Auto-rp group ranges are specifically denied from sparse-mode group range. SSM group range also does not fall under sparse-mode. Link Local multicast groups (224.0.0.0–224.0.0.225, as defined by 224.0.0.0/24) are also denied from the sparse-mode group range. The last entry shows all remaining groups in Sparse-Mode with a given RP.

If multiple RPs are configured with the **pim rp-address** command, then the appropriate group range is displayed with their corresponding RPs. To see the elected RP for a group, specify the group address or name in the **show pim group-map** command.

Examples

The following is sample output form the **show pim group-map** command:

```
ciscoasa# show pim group-map
Group Range      Proto   Client Groups   RP address   Info
224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the PIM Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

The last entry shows that all the remaining groups are in sparse mode mapped to RP 10.10.3.2.

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.
pim rp-address	Configures the address of a PIM rendezvous point (RP).

show pim interface

To display interface-specific information for PIM, use the **show pim interface** command in user EXEC or privileged EXEC mode.

show pim interface [*if_name* | **state-off** | **state-on**]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
state-off	(Optional) Displays interfaces with PIM disabled.
state-on	(Optional) Displays interfaces with PIM enabled.

Command Default

If you do not specify an interface, PIM information for all interfaces is shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The PIM implementation on the ASA considers the ASA itself a PIM neighbor. Therefore, the neighbor count column in the output of this command shows one more than the actual number of neighbors.

Examples

The following example displays PIM information for the inside interface:

```
ciscoasa# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR      DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1       172.16.1.4
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

show pim join-prune statistic

To display PIM join/prune aggregation statistics, use the **show pim join-prune statistics** command in user EXEC or privileged EXEC mode.

show pim join-prune statistics [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Command Default

If an interface is not specified, this command shows the join/prune statistics for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Clear the PIM join/prune statistics with the **clear pim counters** command.

Examples

The following is sample output from the **show pim join-prune statistic** command:

```
ciscoasa# show pim join-prune statistic
PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted              Received
             inside   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
          Ethernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet3   0 /    0 /    0         0 /    0 /    0
   GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
          Ethernet2   0 /    0 /    0         0 /    0 /    0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim neighbor

To display entries in the PIM neighbor table, use the **show pim neighbor** command in user EXEC or privileged EXEc mode.

show pim neighbor [**count | detail**] [*interface*]

Syntax Description

interface	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.
count	(Optional) Displays the total number of PIM neighbors and the number of PIM neighbors on each interface.
detail	(Optional) Displays additional address of the neighbor learned through the upstream-detection hello option.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is used to determine the PIM neighbors known to this router through PIM hello messages. Also, this command indicates that an interface is a designated router (DR) and when the neighbor is capable of bidirectional operation.

The PIM implementation on the ASA considers the ASA itself to be a PIM neighbor. Therefore, the ASA interface is shown in the output of this command. The IP address of the ASA is indicated by an asterisk next to the address.

Examples

The following is sample output from the **show pim neighbor** command:

```
ciscoasa# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the ASA.

show pim range-list

To display range-list information for PIM, use the **show pim range-list** command in user EXEC or privileged EXEC mode.

show pim range-list [*rp_address*]

Syntax Description

rp_address	Can be either one of the following: • Name of the RP, as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4 host** command. • IP address of the RP. This is a multicast IP address in four-part dotted-decimal notation.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable.

Examples

The following is sample output from the **show pim range-list** command:

```
ciscoasa# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

Related Commands

Command	Description
show pim group-map	Displays group-to-PIM mode mapping and active RP information.

show pim topology

To display PIM topology table information, use the **show pim topology** command in user EXEC or privileged EXEC mode.

show pim topology [*group*] [*source*]

Syntax Description

group	(Optional) Can be one of the following: • Name of the multicast group, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
source	(Optional) Can be one of the following: • Name of the multicast source, as defined in the DNS hosts table or with the domain **ipv4 host** command. • IP address of the multicast source. This is a multicast IP address in four-part dotted-decimal notation.

Command Default

Topology information for all groups and sources is shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the MRIB, which is an intermediary for communication between multicast routing protocols, such as PIM, local membership protocols, such as Internet Group Management Protocol (IGMP), and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

Note For forwarding information, use the **show mfib route** command.

Examples

The following is sample output from the **show pim topology** command:

```
ciscoasa# show pim topology
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH
(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH
(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

Related Commands

Command	Description
show mrib route	Displays the MRIB table.
show pim topology reserved	Displays PIM topology table information for reserved groups.

show pim topology reserved

To display PIM topology table information for reserved groups, use the **show pim topology reserved** command in user EXEC or privileged EXEC mode.

show pim topology reserved

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show pim topology reserved** command:

```
ciscoasa# show pim topology reserved
IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR - Sending Registers, E - MSDP External,
    DCC - Don't Check Connected
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Disinterest,
    II - Internal Interest, ID - Internal Disinterest,
    LH - Last Hop, AS - Assert, AB - Admin Boundary
(*,224.0.0.1) L-Local Up: 00:02:26 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  outside            00:02:26  off II
(*,224.0.0.3) L-Local Up: 00:00:48 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags:
  inside             00:00:48  off II
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim topology route-count

To display PIM topology table entry counts, use the **show pim topology route-count** command in user EXEC or privileged EXEC mode.

show pim topology route-count [**detail**]

Syntax Description

detail	(Optional) Displays more detailed count information on a per-group basis.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command displays the count of entries in the PIM topology table. To display more information about the entries, use the **show pim topology** command.

Examples

The following is sample output from the **show pim topology route-count** command:

```
ciscoasa# show pim topology route-count
PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show pim traffic

To display PIM traffic counters, use the **show pim traffic** command in user EXEC or privileged EXEC mode.

show pim traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Clear the PIM traffic counters with the **clear pim counters** command.

Examples

The following is sample output from the **show pim traffic** command:

```
ciscoasa# show pim traffic
PIM Traffic Counters
Elapsed time since counters cleared: 3d06h
                              Received     Sent
Valid PIM Packets                    0       9485
Hello                                0       9485
Join-Prune                           0          0
Register                             0          0
Register Stop                        0          0
Assert                               0          0
Bidir DF Election                    0          0
Errors:
Malformed Packets                               0
Bad Checksums                                   0
Send Errors                                     0
Packet Sent on Loopback Errors                  0
Packets Received on PIM-disabled Interface      0
Packets Received with Unknown PIM Version       0
```

Related Commands

Command	Description
clear pim counters	Clears the PIM traffic counters.

show pim tunnel

To display information about the PIM tunnel interfaces, use the **show pim tunnel** command in user EXEC or privileged EXEC mode.

show pim tunnel [*if_name*]

Syntax Description

if_name	(Optional) The name of an interface. Including this argument limits the displayed information to the specified interface.

Command Default

If an interface is not specified, this command shows the PIM tunnel information for all interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

PIM register packets are sent through the virtual encapsulation tunnel interface from the source first hop DR router to the RP. On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to SM, not SSM and bidirectional PIM.

Examples

The following is sample output from the **show pim tunnel** command:

```
ciscoasa# show pim tunnel
Interface     RP Address Source Address
Encapstunnel0 10.1.1.1   10.1.1.1
Decapstunnel0 10.1.1.1   -
```

Related Commands

Command	Description
show pim topology	Displays the PIM topology table.

show policy-list

To display information about a configured policy list and policy list entries, use the **show policy-list** command in user EXEC or privileged EXEC mode.

show policy-list [*policy_list_name*]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.

Command Default

If you do not specify a policy list name, this command shows all of the policy lists.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Policy lists are used in BGP routing as matching criteria for route maps.

Examples

The following is sample output from the **show policy-list** command:

```
ciscoasa# show policy-list

policy-list policy_list_2 permit
  Match clauses:
    ip address prefix-lists: prefix_1
policy-list policy_list_1 permit
  Match clauses:
    ip address (access-lists): test
    interface inside
```

Related Commands

Command	Description
policy-list	Configures policy lists.

show policy-route

To display the policy-based routing configuration, use the **show policy-route** command in user EXEC or privileged EXEC mode.

show policy-route

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Examples

The following is sample output from the **show policy-list** command:

```
ciscoasa# show policy-route

Interface            Route map
GigabitEthernet0/0   equal-access
```

Related Commands

Command	Description
policy-route	Configures policy-based routing.

show port-channel

To display EtherChannel information in a detailed and one-line summary form or to display the port and port-channel information, use the **show port-channel** command in privileged EXEC mode.

show port-channel [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

Syntax Description

brief	(Default) Shows a brief display.
channel_group_number	(Optional) Specifies the EtherChannel channel group number, between 1 and 48, and only shows information about this channel group.
detail	(Optional) Shows a detailed display.
port	(Optional) Shows information for each interface.
protocol	(Optional) Shows the EtherChannel protocol, such as LACP if enabled.
summary	(Optional) Shows a summary of port-channels.

Command Default

The default is **brief**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Examples

The following is sample output from the **show port-channel** command:

```
ciscoasa# show port-channel
  Channel-group listing:
  -----------------------
Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
```

The following is sample output from the **show port-channel summary** command:

```
ciscoasa# show port-channel summary
Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1             LACP    Gi3/1   Gi3/2   Gi3/3
```

The following is sample output from the **show port-channel detail** command:

```
ciscoasa# show port-channel detail
  Channel-group listing:
  -----------------------
Group: 1
----------
Ports: 3   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: LACP/ active
Minimum Links: 1
Maximum Bundle: 8
Load balance: src-dst-ip
  Ports in the group:
  -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
------------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d

Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
------------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d
Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
```

```
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-----------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x1       0x1     0x304       0x3d
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

The following is sample output from the **show port-channel port** command:

```
ciscoasa# show port-channel port
  Channel-group listing:
  -----------------------
Group: 1
----------
  Ports in the group:
  -------------------
Port: Gi3/1
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-----------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x1       0x1     0x302       0x3d
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/1     SA      bndl       32768         0x0       0x1      0x306       0x3d
Port: Gi3/2
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-----------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x1       0x1     0x303       0x3d
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/2     SA      bndl       32768         0x0       0x1      0x303       0x3d

Port: Gi3/3
------------
Port state    = bndl
Channel group =    1        Mode = LACP/ active
Port-channel  = Po1
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
```

```
Local information:
                             LACP port     Admin     Oper    Port        Port
Port      Flags   State      Priority      Key       Key     Number      State
-----------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x1       0x1     0x304       0x3d
Partner's information:
          Partner Partner    LACP Partner  Partner   Partner  Partner     Partner
Port      Flags   State      Port Priority Admin Key Oper Key Port Number Port State
-----------------------------------------------------------------------------------
Gi3/3     SA      bndl       32768         0x0       0x1      0x302       0x3d
```

The following is sample output from the **show port-channel protocol** command:

```
ciscoasa# show port-channel protocol
  Channel-group listing:
  -----------------------
Group: 1
----------
Protocol: LACP
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.
show lacp	Displays LACP information such as traffic statistics, system identifier, and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

show port-channel load-balance

For EtherChannels, to display the current port-channel load-balance algorithm, and optionally to view the member interface selected for a given set of parameters, enter this command in privileged EXEC mode.

show port-channel *channel_group_number* **load-balance** [**hash-result** { **ip** | **ipv6** | **mac** | **l4port** | **mixed** | **vlan-only** *number* } *parameters*]

Syntax Description

channel_group_number	Specifies the EtherChannel channel group number, between 1 and 48.
hash-result	(Optional) Shows the member interface chosen after hashing values you enter for the current load-balancing algorithm.
ip	(Optional) Specifies IPv4 packet parameters.
ipv6	(Optional) Specifies IPv6 packet parameters.
l4port	(Optional) Specifies port packet parameters.
mac	(Optional) Specifies MAC addresss packet parameters.
mixed	(Optional) Specifies a combination of IP or IPv6 parameters, along with ports and/or the VLAN ID.
parameters	(Optional) Packet parameters, depending on the type. For example, for **ip**, you can specify the source IP address, the destination IP address, and/or the VLAN ID.
vlan-only	(Optional) Specifies the VLAN ID for a packet.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

By default, the ASA balances the packet load on interfaces according to the source and destination IP address (**src-dst-ip**) of the packet. To change the algorithm, see the **port-channel load-balance** command.

This command lets you view the current load-balancing algorithm, but, with the **hash-result** keyword, also lets you test which member interface will be chosen for a packet with given parameters. This command only tests against the current load-balancing algorithm. For example, if the algorithm is src-dst-ip, then enter the IPv4 or IPv6 source and destination IP addresses. If you enter other arguments not used by the current algorithm, they are ignored, and the unentered values actually used by the algorithm default to 0. For example, if the algorithm is vlan-src-ip, then enter:

```
show port-channel 1 load-balance hash-result ip source 10.1.1.1 vlan 5
```

If you enter the following, then the vlan-src-ip algorithm assumes a source IP address of 0.0.0.0 and VLAN 0, and ignores the values you enter:

```
show port-channel 1 load-balance hash-result l4port source 90 destination 100
```

Examples

The following is sample output from the **show port-channel 1 load-balance** command:

```
ciscoasa# show port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
       src-dst-ip
EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
 IPv4: Source XOR Destination IP address
 IPv6: Source XOR Destination IP address
```

The following is sample output from the **show port-channel 1 load-balance hash-result** command, where the entered parameters match the current algorithm (src-dst-ip):

```
ciscoasa# show port-channel 1 load-balance hash-result ip source 10.1.1.1 destination
10.5.5.5
Would select GigabitEthernet2/1 based on algorithm src-dst-ip
```

The following is sample output from the **show port-channel 1 load-balance hash-result** command, where the entered parameters do not match the current algorithm (src-dst-ip), and the hash uses 0 values:

```
ciscoasa# show port-channel 1 load-balance hash-result l4port source 5
Would select GigabitEthernet3/2 of Port-channel1 based on algorithm src-dst-ip
```

Related Commands

Command	Description
channel-group	Adds an interface to an EtherChannel.
interface port-channel	Configures an EtherChannel.
lacp max-bundle	Specifies the maximum number of active interfaces allowed in the channel group.
lacp port-priority	Sets the priority for a physical interface in the channel group.
lacp system-priority	Sets the LACP system priority.
port-channel load-balance	Configures the load-balancing algorithm.
port-channel min-bundle	Specifies the minimum number of active interfaces required for the port-channel interface to become active.

Command	Description
show lacp	Displays LACP information such as traffic statistics, system identifier and neighbor details.
show port-channel	Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information.
show port-channel load-balance	Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters.

show power inline

For models with PoE interfaces, use the **show power inline** command in user EXEC mode to show power status of the interfaces.

show power inline

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Added support for the Firepower 1010.

Usage Guidelines

You can use PoE interfaces to connect devices that require power, such as an IP phone or a wireless access point. For the Firepower 1010, Ethernet 1/7 and 1/8 support PoE+. For the ASA 5505, Ethernet 0/6 and 0/7 support PoE.

Examples

The following is sample output from the **show power inline** command for the Firepower 1010:

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

The following is sample output from the **show power inline** command for the ASA 5505:

```
ciscoasa# show power inline
  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

Table 11-1 shows each field description:

Table 78: show power inline Fields

Field	Description
Interface	Shows all interfaces on the ASA, including ones that do not have PoE available.
Power	Shows whether the power is On or Off. If a device does not need power, if there is no device on that interface, or if the interface is shut down the value is Off. If the interface does not support PoE, then the value is n/a.
Device	(ASA 5505) Shows the type of device obtaining power, either Cisco or IEEE. If the device does not draw power, the value is n/a. The display shows Cisco when the device is a Cisco powered device. IEEE indicates that the device is an IEEE 802.3af- compliant powered device.
Class	(Firepower 1010) Shows the PoE class of the connected device.
Current (mA)	(Firepower 1010) Shows the current being used.
Voltage (V)	(Firepower 1010) Shows the voltage being used.

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.
power inline	Enables or disables PoE.
show interface	Displays the runtime status and statistics of interfaces.

show prefix-list

To display information about configured prefix lists, use the **show prefix-list** command in user EXEC or privileged EXEC mode.

show prefix-list [**summary** | **detail**] [*policy_list_name* [**seq** *sequence_number* | *network/length* [**longer** | **first-match**]]]

Syntax Description

policy_list_name	(Optional) Display information about the specified policy list.
summary	(Optional) Show additional summarized statistical information.
detail	(Optional) Show additional summarized statistical information plus prefix list entries.
seq *sequence_number*	(Optional) Displays only the prefix list entry with the specified sequence number in the specified prefix list.
network/length [**longer** | **first-match**]	(Optional) Displays all entries in the specified prefix list that use this network address and netmask length (in bits). The length of the network mask can be from 0 to 32. You can add these keywords to modify the match: • **longer**—Displays all entries of the specified prefix list that match or are more specific than the given network/length. • **first-match**—Displays the first entry of the specified prefix list that matches the given network/length.

Command Default

If you do not specify a prefix list name, this command shows all of the prefix lists. If you do not include other keywords, the output shows the prefix list entries only.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC or Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Prefix lists are used in routing as matching criteria for route maps and policy lists.

Examples

The following is sample output from the **show prefix-list** command.

```
ciscoasa# show prefix-list

prefix-list prefix_1: 1 entries
   seq 1 permit 2.0.0.0/8
```

The following is an example of summarized output.

```
ciscoasa# show prefix-list summary

Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:   Description: FirstPrefixList
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
```

The following is an example of detailed output.

```
ciscoasa# show prefix-list detail

Prefix-list with the last deletion/insertion: prefix_1
prefix-list prefix_1:   Description: FirstPrefixList
   count: 1, range entries: 0, sequences: 1 - 1, refcount: 3
   seq 1 permit 2.0.0.0/8 (hit count: 0, refcount: 1)
```

Related Commands

Command	Description
prefix-list	Configures prefix lists.

show priority-queue

To display the priority-queue configuration or statistics for an interface, use the **show priority-queue** command in privileged EXEC mode.

show priority-queue { **config | statistics** } [*interface_name*]

Syntax Description

config	Show the queue and TX-ring limits for the interface priority queues.
interface_name	(Optional) Specifies the name of the interface for which you want to show the configuration or the best-effort and low-latency queue statistical details.
statistics	Show the best-effort and low-latency queue statistical details.

Command Default

If you omit the interface name, this command shows the configuration or priority-queue statistics for all configured interfaces.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

This example shows statistics for the interface named test. In the output, BE indicates the best-effort queue, and LLQ represents the low-latency queue:

```
ciscoasa# show priority-queue statistics test
Priority-Queue Statistics interface test
Queue Type        = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
Queue Type        = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
ciscoasa#
```

The following example shows the configuration of the priority queues on all configured interfaces.

```
ciscoasa# show priority-queue config

Priority-Queue Config interface inside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
Priority-Queue Config interface test
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
Priority-Queue Config interface outside
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
Priority-Queue Config interface bgmember1
                current         default         range
queue-limit     0               2048            0 - 2048
tx-ring-limit   4294967295              511             3 - 511
ciscoasa#
```

Related Commands

Command	Description
clear configure priority-queue	Removes the priority-queue configuration from the named interface.
clear priority-queue statistics	Clears the priority-queue statistics counters.
priority-queue	Configures priority queuing on an interface.
show running-config priority-queue	Shows the current priority-queue configuration on the named interface.

show processes

To display a list of the processes that are running on the ASA, use the **show processes** command in privileged EXEC mode.

show processes [**cpu-usage** [[**non-zero**] [**sorted**]] [**cpu-hog | memory | internals**]

Syntax Description

cpu-hog	Shows number and detail of processes that are hogging the CPU (that is, using the CPU for more than 100 milliseconds).
cpu-usage	Shows percentage of CPU used by each process for the last 5 seconds, 1 minute and 5 minutes.
internals	Shows internal details of each process.
memory	Shows memory allocation for each process.
non-zero	(Optional) Shows processes with non-zero CPU usage.
sorted	(Optional) Shows sorted CPU usage for processes.

Command Default

By default, this command displays the processes running on the ASA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.0(4)	The runtime value was enhanced to display accuracy within one millisecond.
7.2(1)	The output was enhanced to display more detailed information about processes that hog the CPU.
8.0(1)	Added the cpu-usage keyword.
9.2(1)	The output was enhanced to display CPU hog detection information.

Usage Guidelines

Processes are lightweight threads that require only a few instructions. The **show processes** commands display a list of the processes that are running on the ASA, as follows:

Command	Data Displayed	Description
show processes	PC	Program counter.
show processes	Stack Pointer	Stack pointer.
show processes	STATE	Address of thread queue.
show processes	Runtime	Number of milliseconds that the thread has been running based on CPU clock cycles. The accurracy is within one millisecond for complete and accurate accounting of process CPU usage based on CPU clock cycles (<10ns resolution) instead of clock ticks (10ms resolution).
show processes	SBASE	Stack base address.
show processes	Stack	Current number of bytes in use and the total size of the stack.
show processes	Process	Function of the thread.
show processes cpu-usage	MAXHOG	Maximum CPU hog runtime in milliseconds.
show processes cpu-usage	NUMHOG	Number of CPU hog runs.
show processes cpu-usage	LASTHOG	Last CPU hog runtime in milliseconds.
show processes cpu-usage	PC	Instruction pointer of the CPU hogging process.
show processes cpu-usage	Traceback	Stack trace of the CPU hogging process. The traceback can have up to 14 addresses.
show processes internals	Invoked Calls	Number of times the scheduler ran the process.
show processes internals	Giveups	Number of times the process yielded the CPU back to the scheduler.

Use the **show processes cpu-usage** command to narrow down a particular process on the ASA that might be using the CPU of the ASA. You can use the **sorted** and **non-zero** commands to further customize the output of the **show processes cpu-usage** command.

With the scheduler and total summary lines, you can run two consecutive **show proccesses** commands and compare the output to determine:

- Consumption of 100% of the CPU.
- Percentage of CPU used by each thread, determined by comparing the runtime delta of a thread to the total runtime delta.

The ASA runs as a single process with many different threads of execution. The output of this command actually shows memory allocations and free memory on a per-thread basis. Because these threads work in cooperation on data flows and other operations pertinent to operation of the ASA, one thread may allocate a block of memory while a different thread may free it. The last row of output contains the total counts over all threads. Only this row may be used to track potential memory leaks by monitoring the difference between allocations and free memory.

Examples

The following example shows how to list processes with non-zero CPU usage. In this example, the ASA 5555 platform uses two DATAPATH threads for packet processing and several control plane processes. The output consolidates the information. The nomenclature for DATAPATH threads are <thread-name>-<core-id>-<process-id> So we know that from output of show process, there are two data path threads running on logical core 0 and 1 with process id 2332 and 2333. If these percentages are high, consider ways to alleviate the load on the machine. For example, if you are running VPN, consider split tunneling or VPN load balancing.

```
ciscoasa# sh processes cpu-usage non-zero
Hardware:   ASA5555
Cisco Adaptive Security Appliance Software Version 9.9(2)56
ASLR enabled, text region 7f83f20fe000-7f83f65ea5cc
PC                   Thread                5Sec     1Min     5Min    Process
0x00007f83f49338b5   0x00002aaac9ead080     0.0%     0.2%     0.2%   vpnfol_thread_timer
0x00007f83f4722e18   0x00002aaac9eddbe0     0.1%     0.0%     0.0%   UserFromCert Thread
0x00007f83f4722e18   0x00002aaac9eae9e0     0.7%     0.4%     0.4%   Unicorn Proxy Thread
0x00007f83f465b6ec   0x00002aaac9ece1c0     0.4%     0.4%     0.4%   Logger
0x00007f83f4272a53   0x00002aaac9ec3b00     0.1%     0.1%     0.1%   Crypto CA
0x00007f83f2f97df9   0x00002aaac9ebcaa0     0.2%     0.2%     0.2%   CP Processing
0x00007f83f52277ed   0x00002aaac9ed1480     0.0%     0.1%     0.0%   Checkheaps
0x00007f83f42c8c83   0x00002aaac9ec3760     0.1%     0.0%     0.0%   CERT API
0x00007f83f347b722   0x00002aaac9eb7740     0.1%     0.1%     0.1%   ARP Thread
                 -                  -      37.1%    36.8%    36.3%   DATAPATH-0-2332
                 -                  -      37.2%    36.8%    36.3%   DATAPATH-1-2333
```

The following example shows how to display a list of processes that are running on the ASA:

```
ciscoasa#  show processes
    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->
-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total
```

The following example shows how to display the percentage of CPU used by each process:

```
ciscoasa# show proc cpu-usage non-zero

PC    Thread    5Sec   1Min   5Min   Process
0818af8e    d482f92c    0.1%   0.1%   0.1%   Dispatch Unit
08bae136    d48180f0    0.1%   0.0%   0.2%   ssh
--------------------------------------
```

The following examples show how to display the number and detail of processes that are hogging the CPU:

```
ciscoasa# show processes cpu-hog
 Granular CPU hog detection currently running, started at 15:41:16 UTC Jan 6 2014.
 Sample count: 10000 Threshold: 10ms
 Granular CPU hog detection completed at 15:41:16 UTC Jan 6 2014.
 Sample count: 10000 Threshold: 10ms
 The remainder of the CPU hog traceback follows:
 Process: DATAPATH-0-2042, NUMHOG: 430, MAXHOG: 22, LASTHOG: 2
 LASTHOG At: 15:42:21 UTC Jan 6 2014
 PC: 0x0000000000000000 (suspend)
 Call stack: 0x000000000041c98c 0x000000000041cc99 0x000000000069b0f0
 0x00000000013619af 0x000000000136cbbd 0x0000000001372203
 0x00007ffffeab2f3a
 Interrupt based hog #1
 Hog #1, traceback #1, at: 15:41:16 UTC Jan 6 2014, hog 20 ms
 PC: 0x0000000000eb616b
 Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x0000000000ebcf71
 0x0000000000ebc5ab 0x0000000000ebcb0e 0x0000000000e17410
 0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
 0x0000000001344419 0x000000000069b315 0x000000000069be9e
 0x000000000069b0a4 0x00000000013619af
 Hog #1, traceback #2, at: 15:41:16 UTC Jan 6 2014, hog 21 ms
 PC: 0x0000000000e8fc41
 Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x0000000000e17410
 0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
 0x0000000001344419 0x000000000069b315 0x000000000069be9e
 0x000000000069b0a4 0x00000000013619af 0x000000000136cbbd
 0x0000000001372203 0x00007ffffeab2f3a
 Interrupt based hog #2
 Hog #2, traceback #1, at: 15:41:36 UTC Jan 6 2014, hog 9 ms
 PC: 0x0000000000eb6167
 Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x0000000000ebcf71
 0x0000000000ebc5ab 0x0000000000ebcb0e 0x0000000000e17410
 0x0000000000e19ac4 0x0000000000e19e55 0x0000000000ca50b4
 0x0000000001344419 0x000000000069b315 0x000000000069be9e
 0x000000000069b0a4 0x00000000013619af
 Interrupt based hog #3
 Hog #3, traceback #1, at: 15:42:21 UTC Jan 6 2014, hog 2 ms
 PC: 0x000000000068a223
 Call stack: 0x0000000001360281 0x00007ffffeaba5f0 0x000000000069bbba
 0x000000000069b0a4 0x00000000013619af 0x000000000136cbbd
 0x0000000001372203 0x00007ffffeab2f3a
```

The following example shows how to display the memory allocation for each process:

```
ciscoasa# show processes memory

 ------------------------------------------------------------
 Allocs Allocated Frees Freed Process
 (bytes) (bytes)
 ------------------------------------------------------------
 23512 13471545 6 180 *System Main*
 0 0 0 0 lu_rx
 2 8324 16 19488 vpnlb_thread
```

The following example shows how to display the internal details of each process:

```
ciscoasa# show processes internals
Invoked Giveups Process
 1 0 block_diag
 19108445 19108445 Dispatch Unit
 1 0 CF OIR
 1 0 Reload Control Thread
 1 0 aaa
 2 0 CMGR Server Process
 1 0 CMGR Timer Process
 2 0 dbgtrace
 69 0 557mcfix
 19108019 19108018 557poll
 2 0 557statspoll
 1 0 Chunk Manager
 135 0 PIX Garbage Collector
 6 0 route_process
 1 0 IP Address Assign
 1 0 QoS Support Module
 1 0 Client Update Task
 8973 8968 Checkheaps
 6 0 Session Manager
 237 235 uauth
(other lines deleted for brevity)
```

Related Commands

Command	Description
show cpu	Shows the CPU usage information.

show ptp

To display a variety of PTP statistics and clock-related information, use the **show ptp** command in privileged EXEC or global configuration mode.

show ptp { **clock** | **internal-info** | **port** [*interface-name*] }

Note This command applies only to the Cisco ISA 3000 appliance.

Syntax Description

clock	Displays PTP clock properties.
internal-info	Displays PTP internal information, including port-specific counters.
port	Displays PTP port information for all PTP-enabled interfaces.
interface-name	Shows PTP port information for the specified interface.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.7(1)	This command was added.

Usage Guidelines

If you include the optional interface ID in the **show ptp port** command, the port information for only that interface is shown.

The **show ptp clock | port | internal-info** commands are also available in global configuration mode.

Examples

The following example shows PTP clock properties:

```
ciscoasa# show ptp clock
PTP CLOCK INFO
  PTP Device Type: Transparent Clock
  Operation mode: One Step
  Clock Identity: 0:8:2F:FF:FE:E8:43:81
  Clock Domain: 0
  Number of PTP ports: 4
```

The following example shows PTP port information for all PTP-enabled interfaces:

```
ciscoasa# **show ptp port**
PTP PORT DATASET: GigabitEthernet1/1
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 1
  PTP version: 2
  Port state: Enabled
PTP PORT DATASET: GigabitEthernet1/2
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 2
  PTP version: 2
  Port state: Disabled
PTP PORT DATASET: GigabitEthernet1/3
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 3
  PTP version: 2
  Port state: Disabled
PTP PORT DATASET: GigabitEthernet1/4
  Port identity: clock identity: 0:8:2F:FF:FE:E8:43:81
  Port identity: port number: 4
  PTP version: 2
  Port state: Enabled
```

show quota management-session

To show statistics for the current management session:, use the **show quota management-session** command in privileged EXEC mode.

show quota management-session [**ssh** | **telnet** | **http** | **username** *user*]

Syntax Description

ssh	Shows SSH sessions.
telnet	Shows Telnet sessions.
http	Shows HTTP sessions.
username *user*	Shows sessions for a given user.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(2)	This command was added.
9.12(1)	This command is now only available within a context, because the **quota management-session** command now supports quotas per context. Added the **ssh**, **telnet**, **http**, and **username** keywords. The display output now shows the number of sessions per protocol.

Usage Guidelines

This command shows the active administrative sessions by type.

Examples

The following example shows statistics for the current management session:

```
ciscoasa# show quota management-session
#Sessions            ConnectionType              Username
1                           SSH                  cisco
2                           TELNET               cisco
1                           SSH                  cisco1
```

Related Commands

Command	Description
show running-config quota management-session	Shows the current value of the management session quota.
quota management-session	Sets the number of simultaneous ASDM, SSH, and Telnet sessions allowed on the device.

show raid

To display information about RAID status for the hard drives in the system, use the **show raid** command in privileged EXEC mode.

show raid

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.1(1)	This command was added.
9.17(1)	Support for the Secure Firewall 3100 was added.

Usage Guidelines

Some hardware models support two internal hard drives. For example, the ASA 5545-X and 5555-X support up to two solid state drives. When two drives are present, they are automatically formatted in a RAID-1 configuration. This structure is rebuilt every time you reload the device. You can use the **show raid** command to view information about the RAID configuration.

Note If a device model does not support RAID, you might get an invalid command error message when you enter the **show raid** command.

Examples

The following sample display shows two SSDs in the RAID on the Secure Firewall 3100:

```
> show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  operable
Presence:                     equipped
Lifecycle:                    available
Drive State:                  optimal
Type:                         raid
Level:                        raid1
Max Disks:                    2
```

```
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

The following sample display shows one SSD in the RAID; disk2 is not present, and the RAID is shown as "degraded:"

```
> show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

The following example for an ASA device shows that there is one active, working hard drive device, as shown by the State, Active Devices, and Working Devices lines. The output also shows that the second device is “removed,” as shown in the final table. This means either that no second drive was installed, or that the second drive has actually been removed.

```
ciscoasa# show raid
```

```
/dev/md0:
        Version : 1.2
  Creation Time : Mon Mar  6 09:04:14 2017
     Raid Level : raid1
     Array Size : 124969216 (119.18 GiB 127.97 GB)
  Used Dev Size : 124969216 (119.18 GiB 127.97 GB)
   Raid Devices : 2
  Total Devices : 1
    Persistence : Superblock is persistent
  Intent Bitmap : Internal
    Update Time : Tue Mar 21 14:03:27 2017
          State : active, degraded
 Active Devices : 1
Working Devices : 1
 Failed Devices : 0
  Spare Devices : 0
           Name : ciscoasa:0  (local to host ciscoasa)
           UUID : e8f90a6b:20433f38:e8b86378:6fd52057
         Events : 454610
    Number   Major   Minor   RaidDevice State
       0       8       0        0      active sync   /dev/sda
       1       0       0        1      removed
```

The following table explains the fields in the output.

Field	Description
Identifier	The array component identifier; for example, /dev/md0.
Version	The format of the Superblock (RAID metadata).
Creation Time	The date and time when this component was configured.
Raid Level	The raid level. RAID1 is a mirroring scheme.
Array Size	The total storage space available across all component devices in bytes (as well as gibibytes and gigabytes).
Used Dev Size	The amount of storage space contributed to the total by each device in bytes (as well as gibibytes and gigabytes). This is determined by the smallest device or partition; there may be unused space on larger devices.
RAID Devices	The total number of member devices in the complete array, including spare, missing, and failed devices.
Total Devices	The number of functional devices available.
Persistence	A persistent Superblock (the default when an array is created) means the Superblock is written to a specific location in all component devices of the array. The RAID configuration can then be read directly from the disks involved.
Update Time	The time at which the array status changed. Status changes include activation, failure, etc.

Field	Description
State	The current status of RAID. The first status indicates **active** if the array is fully operational, or **clean** if the array is active but there are no pending write operations. The possible statuses are: • active, resyncing—The system is new and it is currently building the RAID structure. It can take over 90 minutes to build the required structure. Look for a Rebuild Status line in the output, which indicates the percentage completed. • (clean or active), degraded, recovering—The RAID structure has been built successfully. • (clean or active), degraded—One hard drive is not functioning. It is either broken or missing. If you intend to have two drives, replace the broken or missing drive. • (clean or active), degraded, recovering—The system is in the process of rebuilding the RAID structure after installing or replacing a hard drive.
Active Devices	The number of currently functioning devices in the array; does not include spare devices.
Working Devices	The total number of operational (non-failed) devices in the array; that is, active devices plus spare devices.
Failed Devices	The number of failed devices in the array.
Spare Devices	The number of spare devices currently assigned to the array. If the array is missing a member, an available spare should get built into the array as an active member. But a drive can also be marked spare if the system failed to add it to the array.
UUID	The 128-bit hexadecimal universally unique identifier (UUID) stored in the array's Superblock. This number is randomly generated and used to uniquely tag a RAID. All component devices share this ID.
Events	Event counter for the array; incremented whenever the Superblock is updated.
Component table.	Component disks are numbered from 0. The Major number usually corresponds to the device type, while the Minor number is the identifier for a specific device in that group. For example, Major 8 indicates a SCSI disk. Each component of the RAID device is listed here, with the components current status. A healthy disk is in the **active sync** state.

show reload

To display the reload status on the ASA, use the **show reload** command in privileged EXEC mode.

show reload

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

This command has no usage guidelines.

Examples

The following example shows that a reload is scheduled for 12:00 a.m. (midnight) on Saturday, April 20:

```
ciscoasa# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

Related Commands

Command	Description
reload	Reboots and reloads the configuration.

show resource allocation

To show the resource allocation for each resource across all classes and class members, use the **show resource allocation** command in privileged EXEC mode.

show resource allocation [**detail**]

Syntax Description

detail	Shows additional information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.0(1)	A new resource class, routes, was created to set the maximum number of routing table entries in each context. New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Usage Guidelines

This command shows the resource allocation, but does not show the actual resources being used. See the **show resource usage** command for more information about actual resource usage.

Examples

The following is sample output from the **show resource allocation** command. The display shows the total allocation of each resource as an absolute value and as a percentage of the available system resources.

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
 Syslogs [rate]             10500           N/A
 Conns                     305000           30.50%
 Hosts                      78842           N/A
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Routes                     25000           0.00%
 Xlates                     91749           N/A
 Other VPN Sessions            20           2.66%
 Other VPN Burst              20           2.66%
 All                   unlimited
```

Table 11-2 shows each field description.

Table 79: show resource allocation Fields

Field	Description
Resource	The name of the resource that you can limit.
Total	The total amount of the resource that is allocated across all contexts. The amount is an absolute number of concurrent instances or instances per second. If you specified a percentage in the class definition, the ASA converts the percentage to an absolute number for this display.
% of Avail	The percentage of the total system resources that is allocated across all contexts, if available. If a resource does not have a system limit, this column shows N/A.

Examples

The following is sample output from the **show resource allocation detail** command:

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource          Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]      default          all      CA  unlimited
                  gold               1       C      34000      34000     N/A
                  silver             1      CA      17000      17000     N/A
                  bronze             0      CA       8500
                  All Contexts:      3                         51000     N/A
Inspects [rate]   default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      10000      10000     N/A
                  bronze             0      CA       5000
                  All Contexts:      3                         10000     N/A
Syslogs [rate]    default          all      CA  unlimited
                  gold               1       C       6000       6000     N/A
                  silver             1      CA       3000       3000     N/A
                  bronze             0      CA       1500
                  All Contexts:      3                          9000     N/A
Conns             default          all      CA  unlimited
                  gold               1       C     200000     200000     20.00%
                  silver             1      CA     100000     100000     10.00%
                  bronze             0      CA      50000
                  All Contexts:      3                        300000     30.00%
Hosts             default          all      CA  unlimited
                  gold               1      DA  unlimited
                  silver             1      CA      26214      26214      N/A
                  bronze             0      CA      13107
                  All Contexts:      3                         26214      N/A
SSH               default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
                  bronze             0      CA          5
                  All Contexts:      3                            20     20.00%
Telnet            default          all       C          5
                  gold               1       D          5          5      5.00%
                  silver             1      CA         10         10     10.00%
```

```
                 bronze           0      CA          5
                 All Contexts:    3                            20     20.00%
Routes           default        all       C  unlimited                  N/A
                 gold             1       D  unlimited          5       N/A
                 silver           1      CA         10         10       N/A
                 bronze           0      CA          5                  N/A
                 All Contexts:    3                            20       N/A
Xlates           default        all      CA  unlimited
                 gold             1      DA  unlimited
                 silver           1      CA      23040      23040     N/A
                 bronze           0      CA      11520
                 All Contexts:    3                         23040     N/A
mac-addresses    default        all       C      65535
                 gold             1       D      65535      65535    100.00%
                 silver           1      CA       6553       6553      9.99%
                 bronze           0      CA       3276
                 All Contexts:    3                        137623    209.99%
```

Table 11-3 shows each field description.

Table 80: show resource allocation detail Fields

Field	Description
Resource	The name of the resource that you can limit.
Class	The name of each class, including the default class. The All contexts field shows the total values across all classes.
Mmbrs	The number of contexts assigned to each class.
Origin	The origin of the resource limit, as follows: • A—You set this limit with the **all** option, instead of as an individual resource. • C—This limit is derived from the member class. • D—This limit was not defined in the member class, but was derived from the default class. For a context assigned to the default class, the value will be “C” instead of “D.” The ASA can combine “A” with “C” or “D.”
Limit	The limit of the resource per context, as an absolute number. If you specified a percentage in the class definition, the ASA converts the percentage to an absolute number for this display.
Total	The total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.
% of Avail	The percentage of the total system resources that is allocated across all contexts in the class, if available. If the resource is unlimited, this display is blank. If the resource does not have a system limit, this column shows N/A.

Related Commands

Command	Description
class	Creates a resource class.

Command	Description
context	Adds a security context.
limit-resource	Sets the resource limit for a class.
show resource types	Shows the resource types for which you can set limits.
show resource usage	Shows the resource usage of the ASA.

show resource types

To view the resource types for which the ASA tracks usage, use the **show resource types** command in privileged EXEC mode.

show resource types

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command shows additional resource types that you can manage for each context.
9.0(1)	A new resource class, routes, was created to set the maximum number of routing table entries in each context. New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Examples

The following sample display shows the resource types:

```
ciscoasa# show resource types
Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec
Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  Routes          Routing Table Entries
  Other-vpn       Other VPN licenses
  Other-vpn-burst Allowable burst for Other VPN licenses
  All             All Resources
```

Related Commands

Command	Description
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
show resource usage	Shows the resource usage of the ASA.

show resource usage

To view the resource usage of the ASA or for each context in multiple mode, use the **show resource usage** command in privileged EXEC mode.

show resource usage [**context** *context_name* | **top** *n* **| all | summary | system | detail**] [**resource** { [**rate**] *resource_name* | **all** }] [**counter** *counter_name* [*count_threshold*]]

Syntax Description

context *context_name*	(Multiple mode only) Specifies the context name for which you want to view statistics. Specify **all** for all contexts; the ASA lists the context usage for each context.
count_threshold	Sets the number above which resources are shown. The default is 1. If the usage of the resource is below the number you set, then the resource is not shown. If you specify **all** for the counter name, then the *count_threshold* applies to the current usage. **Note** To show all resources, set the *count_threshold* to **0** .
counter *counter_name*	Shows counts for the following counter types: • **current** —Shows the active concurrent instances or the current rate of the resource. • **peak** —Shows the peak concurrent instances, or the peak rate of the resource since the statistics were last cleared, either using the **clear resource usage** command or because the device rebooted. • **denied** —Shows the number of instances that were denied because they exceeded the resource limit shown in the Limit column. • **all** —(Default) Shows all statistics.
detail	Shows the resource usage of all resources, including those you cannot manage. For example, you can view the number of TCP intercepts.

resource [**rate**] *resource_name*	Shows the usage of a specific resource. Specify **all** (the default) for all resources. Specify **rate** to show the rate of usage of a resource. Resources that are measured by rate include **conns** , **inspects** , and **syslogs** . You must specify the **rate** keyword with these resource types. The conns resource is also measured as concurrent connections; only use the **rate** keyword to view the connections per second. Resources include the following types: • **asdm** —ASDM management sessions. • **conns** —TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. • **inspects** —Application inspections. • **hosts** —Hosts that can connect through the ASA. • **mac-address es** —For transparent firewall mode, the number of MAC addresses allowed in the MAC address table. • **routes—** Routing Table entries. • **ssh** —SSH sessions. • **syslogs** —System log messages. • **telnet** —Telnet sessions. • (Multiple mode only) **VPN Other** —Site-to-site VPN sessions. • (Multiple mode only) **VPN Burst Other** —Site-to-site VPN burst sessions. • **xlates** —NAT translations.
summary	(Multiple mode only) Shows all context usage combined.
system	(Multiple mode only) Shows all context usage combined, but shows the system limits for resources instead of the combined context limits.
top *n*	(Multiple mode only) Shows the contexts that are the top *n* users of the specified resource. You must specify a single resource type, and not **resource** **all** , with this option.

Command Default

For multiple context mode, the default context is **all** , which shows resource usage for every context. For single mode, the context name is ignored and the output shows the “context” as “System.”

The default resource name is **all** , which shows all resource types.

The default counter name is **all** , which shows all statistics.

The default count threshold is **1** .

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	This command shows the denied resources, because you can limit the resources for each context.
9.0(1)	A new resource class, routes, was created to set the maximum number of routing table entries in each context. New resource types, vpn other and vpn burst other, were created to set the maximum number of site-to-site VPN tunnels in each context.

Examples

The following is sample output from the **show resource usage context** command, which shows the resource usage for the admin context:

```
ciscoasa# show resource usage context admin
Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

The following is sample output from the **show resource usage summary** command, which shows the resource usage for all contexts and all resources. This sample shows the limits for six contexts.

```
ciscoasa# show resource usage summary
Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
Other VPN Sessions          0           10         10        740 Summary
Other VPN Burst             0           10         10        730 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

The following is sample output from the **show resource usage system** command, which shows the resource usage for all contexts, but it shows the system limit instead of the combined context limits:

```
ciscoasa# show resource usage system
Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

The following is sample output from the **show resource usage detail counter all 0** command, which shows all resources, and not only those you can manage:

```
ciscoasa# show resource usage detail counter all 0
Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
chunk:dhcp-lease-s          0            0  unlimited             0 admin
chunk:dnat                  0            0  unlimited             0 admin
chunk:ether                 0            0  unlimited             0 admin
chunk:est                   0            0  unlimited             0 admin
...
Telnet                      0            0          5             0 admin
SSH                         1            1          5             0 admin
ASDM                        0            1          5             0 admin
Syslogs [rate]              0           68  unlimited             0 admin
aaa rate                    0            0  unlimited             0 admin
url filter rate             0            0  unlimited             0 admin
Conns                       1            6  unlimited             0 admin
Xlates                      0            0  unlimited             0 admin
tcp conns                   0            0  unlimited             0 admin
Hosts                       2            3  unlimited             0 admin
Other VPN Sessions          0           10        750           740 admin
Other VPN Burst             0           10        750           730 admin
udp conns                   0            0  unlimited             0 admin
smtp-fixups                 0            0  unlimited             0 admin
Conns [rate]                0            7  unlimited             0 admin
establisheds                0            0  unlimited             0 admin
pps                         0            0  unlimited             0 admin
syslog rate                 0            0  unlimited             0 admin
bps                         0            0  unlimited             0 admin
Fixups [rate]               0            0  unlimited             0 admin
non tcp/udp conns           0            0  unlimited             0 admin
tcp-intercepts              0            0  unlimited             0 admin
globals                     0            0  unlimited             0 admin
np-statics                  0            0  unlimited             0 admin
statics                     0            0  unlimited             0 admin
nats                        0            0  unlimited             0 admin
ace-rules                   0            0        N/A             0 admin
aaa-user-aces               0            0        N/A             0 admin
filter-rules                0            0        N/A             0 admin
est-rules                   0            0        N/A             0 admin
aaa-rules                   0            0        N/A             0 admin
console-access-rul          0            0        N/A             0 admin
policy-nat-rules            0            0        N/A             0 admin
fixup-rules                 0            0        N/A             0 admin
aaa-uxlates                 0            0  unlimited             0 admin
CP-Traffic:IP               0            0  unlimited             0 admin
CP-Traffic:ARP              0            0  unlimited             0 admin
CP-Traffic:Fixup            0            0  unlimited             0 admin
CP-Traffic:NPCP             0            0  unlimited             0 admin
CP-Traffic:Unknown          0            0  unlimited             0 admin
```

Related Commands

Command	Description
class	Creates a resource class.
clear resource usage	Clears the resource usage statistics
context	Adds a security context.
limit-resource	Sets the resource limit for a class.
show resource types	Shows a list of resource types.

show rest-api agent

To determine if the REST API Agent is currently enabled, use the **show rest-api agent** command in privileged EXEC mode.

show rest-api agent

Note This command is supported on all versions of ASA virtual, the ASA 5585-X, and all ASA 5500-X series devices except the ASA 5506-X and ASA 5508-X.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

Use this command to determine if the REST API Agent is currently enabled.

Examples

This example indicates that the REST API Agent is enabled:

```
ciscoasa(config)# show rest-api agent
REST API agent is currently enabled.
```

If the Agent is disabled, the message displayed is “REST API agent is currently disabled.”

Related Commands

Commands	Description
rest-api	Verify and install the REST API package. Enable the REST API Agent.
show version	If the REST API Agent is enabled, its version number is included in **show version** output.

show rip database

To display the information that is stored in the RIP topological database, use the **show rip database** command in privileged EXEC mode.

show rip database [*ip_addr* [*mask*]]

Syntax Description

ip_addr	(Optional) Limits the display routes for the specified network address.
mask	(Optional) Specifies the network mask for the optional network address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The RIP routing-related **show** commands are available in privileged EXEC mode on the ASA. You do not need to be in an RIP configuration mode to use the RIP-related **show** commands.

The RIP database contains all of the routes learned through RIP. Routes that appear in this database may not necessarily appear in the routing table. See the *Cisco Security Appliance Command Line Configuration Guide* for information about how the routing table is populated from the routing protocol databases.

Examples

The following is sample output from the **show rip database** command:

```
ciscoasa# show rip database
10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
 [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

The following is sample output from the **show rip database** command with a network address and mask:

```
Router# show rip database 172.19.86.0 255.255.255.0
172.19.86.0/24
```

```
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

Related Commands

Command	Description
router rip	Enables RIP routing and configures global RIP routing parameters.

show rollback-status

When Cisco Security Manager sends a rollback request to ASA, the management connection from Cisco Security Manager to ASA is reset; the result of the rollback job cannot be sent to Cisco Security Manager. Use **show rollback-status** to display the status of rollback job to Cisco Security Manager when it queries ASA.

show rollback-status [*context_name*]

Syntax Description

context_name	The name of the context for which the rollback job is applied to. For single mode, this is not applicable.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Config	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.6(3)	This command was introduced.

Usage Guidelines

Use **show rollback-status** to display the status of rollback job, start, end time and context name the rollback job applied to.

Examples

The following examples show the rollback status for all contexts, entered in single mode:

1. Before any rollback request is received from Cisco Security Manager:

```
ciscoasa(config)# sh rollback-status
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. When first rollback request is received on ASA, before the job is completed:

```
ciscoasa(config)# sh rollback-status
Status      : In Progress
Start Time  : 13:00:12 UTC May 11 2017
End Time    : N/A
```

3. When the rollback job is completed:

```
ciscoasa(config)# sh rollback-status
```

```
Status      : Succeeded
Start Time  : 13:00:12 UTC May 11 2017
End Time    : 13:00:14 UTC May 11 2017
```

4. If the rollback failed, its output would be:

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Failed
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

5. If the rollback failed, and it reverts to the startup config:

```
ciscoasa(cfg-cluster)# sh rollback-status
Status      : Reverted ( Roll back failed, startup config applied )
Start Time  : 13:25:49 UTC May 11 2017
End Time    : 13:25:55 UTC May 11 2017
```

The following examples show the rollback status entered in multiple mode and from system/admin context:

1. Before any rollback deployed into ASA:

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

2. When the rollback on system context started:

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : In Progress
Start Time  : 16:55:35 UTC May 11 2017
End Time    : N/A
Context Name: admin
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

3. When the Rollback on system context is completed:

```
ciscoasa(config)# sh rollback-status
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
Context Name: ctx1
Status      : None
Start Time  : N/A
End Time    : N/A
Context Name: ctx2
Status      : None
Start Time  : N/A
End Time    : N/A
```

4. When context name is specified in the command:

```
ciscoasa(config)# sh rollback-status system
Context Name: system
Status      : Succeeded
Start Time  : 19:52:25 UTC May 11 2017
End Time    : 19:52:34 UTC May 11 2017
ciscoasa(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

The following examples show the rollback status entered in multiple mode and from admin/user context:

1. When no context name is specified:

```
ciscoasa/admin(config)# sh rollback-status
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

2. When context name is specified:

```
ciscoasa/admin(config)# sh rollback-status admin
Context Name: admin
Status      : Succeeded
Start Time  : 19:55:26 UTC May 11 2017
End Time    : 19:55:26 UTC May 11 2017
```

3. When incorrect context name is specified

```
ciscoasa/admin(config)# sh rollback-status ad
Context ad does not exist.
```

4. When the context name does not match current context:

```
ciscoasa/admin(config)# sh rollback-status ctx1
Context ctx1 does not match current context.
```

When ASA is running as Slave or Standby unit, a warning message is displayed.

1. When the show command is issued from Slave, the output would be:

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Slave.
```

2. When the show command issued from standby, the output would be:

```
ciscoasa(config)# sh rollback-status
WARNING: Current unit is Standby.
```

The following table describes the output entries in detail.

Output	**Description**
Context Name	The name of the context for which the rollback job is applied to. For single mode, this is not displayed.
Status	The status of the most recent rollback job. It can be any one of the following: • None—No rollback job has been ever deployed to this context. • In Progress—ASA has received the rollback request from Cisco Security Manager, and the rollback job is in progress. • Succeeded—The rollback has completed successfully. • Reverted—Rollback to the configure sent from Cisco Security Manager failed, rollback to the startup configure saved on the ASAis triggered, and this revert action is completed successfully, and now ASA is running the startup config. • Failed—Rollback completed with error.
Start Time	The start time for most recent rollback job. Whenever a rollback job is received on ASA, this field is updated with the current time on ASA; the Status is updated as “In Progress”. If rollback is in None state, “N/A” is displayed.
End Time	The time when rollback job is completed. If the job is completed without error, the “Status” is updated as “Succeeded”. If revert action has been taken during rollback, and revert is completed successfully, the status is updated as “Reverted”. If revert failed, the status is updated as “Failed”. For rollback in “None” or “In Progress” state, “N/A” is displayed.

show route

To display the routing table, use the **show route** command in privileged EXEC mode.

The parameters you can use with this command differ depending on the firewall mode of the device, routed or transparent. This is indicated in the syntax description.

show route [**management-only** [*interface_name*]] [**cluster | failover |** *hostname* | *ip_address* [*mask*] [**longer-prefixes**] | **domain-name** *hostname_or_ip_address* | **bgp** [*as_number*] **| connected | eigrp** [*process_id*] **| isis | isis | ospf** [*process_id*] **| rip | static | summary | zone**]

Syntax Description

bgp *as_number*	(Routed.) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number) for the BGP route. The *as_number* limits the display to route entries that use the specified AS number.
cluster	(Routed.) Displays the routing information base (RIB) epoch number (sequence number), the current timer value, and the network descriptor block epoch number (sequence number).
connected	(Routed, transparent.) Displays connected routes.
domain-name *hostname_or_ip_address*	(Routed, transparent.) Displays routes to the specified destination hostname. You must configure DNS for hostname resolution to work. You can also use an IP address on this keyword.
eigrp *process_id*	(Routed.) Displays EIGRP routes.
failover	(Routed.) Displays the current sequence number of the routing table and routing entries after failover has occurred, and a standby unit becomes the active unit.
hostname	(Routed, transparent.) Displays routes to the specified destination hostname. You must configure DNS for hostname resolution to work.
interface_name	(Routed, transparent.) Displays route entries that use the specified interface.
ip_address mask	(Routed, transparent.) Displays routes to the specified destination.
isis	(Routed.) Displays IS-IS routes.
longer-prefixes	(Routed, transparent.) Displays routes that match the specified *ip_address* /*mask* pair only
management-only	(Routed, transparent.) Displays routes in the IPv4 management routing table.
isis	(Routed.) Displays IS-IS routes.
ospf *process_id*	(Routed.) Displays OSPF routes.
rip	(Routed.) Displays RIP routes.
static	(Routed, transparent.) Displays static routes.

summary	(Routed, transparent.) Displays the current state of the routing table.
zone	(Routed, transparent.) Displays the routes for zone interfaces.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.0(2)	The **eigrp** keyword was added.
8.4(1)	The **failover** keyword was added. The output shows the RIB epoch number (sequence number), current timer value, and network descriptor block epoch number (sequence number).
9.0(1)	The **cluster** keyword was added. Applies to the dynamic routing protocols (EIGRP, OSPF, and RIP) and is only available on the ASA 5580 and 5585-X.
9.2(1)	The **bgp** keyword was added.
9.2(1)	The command now displays the local host routes, along with **connected** routes. New codes (L, I, E, su and +) are added to indicate the protocol or type of route being displayed.
9.3(2)	The **zone** keyword was added.
9.5(1)	Support for the management routing table feature was added.
9.6(1)	We added the **isis** keyword.
9.6(1)	The **isis** keyword was added.
9.20(2)	The **domain-name** keyword was added.

Usage Guidelines

The **show route** command provides output similar to the **show ipv6 route** command, except that the information is IPv4-specific.

Note The **clustering** and **failover** keywords do not appear unless these features are configured on the ASA.

The **show route** command lists the "best" routes for new connections. When you send a permitted TCP SYN to the backup interface, the ASA can only respond using the same interface. If there is no default route in the

RIB on that interface, the ASA drops the packet because of no adjacency. Everything that is configured as shown in the **show running-config route** command is maintained in certain data structures in the system.

You can check the backend interface-specific routing table with the **show asp table routing** command. This design is similar to OSPF or EIGRP, in which the protocol-specific route database is not the same as the global routing table, which only displays the "best" routes. This behavior is by design.

Note When you use the **show ip route** command in the Cisco IOS, the **longer-prefix** keyword is available. When you use this keyword in the Cisco IOS, the route is only displayed if the specified network and mask pair match. On the ASA, the **longer-prefix** keyword is the default behavior for the **show rout** e command; that is, no additional keyword is needed in the CLI. Because of this, you cannot see the route when you type **ip** . To obtain the supernet route, the mask value needs to be passed with the IP address.

Examples

The following is sample output from the **show route** command:

```
ciscoasa# show route
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route
Gateway of last resort is 10.86.194.1 to network 0.0.0.0
C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

The following is sample output of the **show route** command on the ASA 5555, in the admin context. The output displays the internal loopback address, which is used by the VPN hardware client for individual user authentication.

```
ciscoasa/admin(config)# show route
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route
Gateway of last resort is 10.86.194.1 to network 0.0.0.0
C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

The following is sample output from the **show route bgp** command:

```
ciscoasa# show route bgp
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is 10.86.116.1 to network 0.0.0.0
```

The following is sample output of the **show route failover** command, which shows the synchronization of OSPF and EIGRP routes to the standby unit after failover:

```
ciscoasa(config)# show route failover
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route
Gateway of last resort is 10.86.194.1 to network 0.0.0.0
Routing table sequence number 1
Reconvergence timer 00.20 (Running)
S    10.10.10.0 255.0.0.0 [1/0] via 10.10.10.1, mgmt, seq 1
                      [1/0] via 10.10.10.2, mgmt, seq 1
D    209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 0
D   10.65.68.220 255.255.255.255 [1/0] via 10.76.11.1, mgmt, seq 1
```

The following is sample output from the **show route cluster** command:

```
ciscoasa(cfg-cluster)# show route cluster
Codes: L - Local, C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, E - EGP, EX - EIGRP external, O - OSPF, I - IGRP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, su - IS-IS summary, U - per-user static route, o - ODR
       P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set
Routing table seq num 2
Reconvergence timer expires in 52 secs
C    70.0.0.0 255.255.255.0 is directly connected, cluster, seq 1
C    172.23.0.0 255.255.0.0 is directly connected, tftp, seq 1
C    200.165.200.0 255.255.255.0 is directly connected, outside, seq 1
C    198.51.100.0 255.255.255.0 is directly connected, inside, seq 1
O   198.51.100.0 255.255.255.0 [110/28416] via 198.51.100.10, 0:24:45, inside, seq 2
D   209.165.200.224 255.255.255.0 [90/28416] via 200.165.200.225, 0:00:15, outside, seq 2
```

The following is sample output from the **show route summary** command:

```
ciscoasa# show route summary
IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          1           0           0           88          288
bgp 2           0           0           0           0           0
  External: 0 Internal: 0 Local: 0
internal        1                                               408
Total           2           2           0           264         1272
```

See the following output for the **show route zone** command:

```
ciscoasa# show route zone
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is not set
S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

The following example shows output from the **show route isis** command.

```
ciscoasa# show route isis
Routing Table:
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set
i L2     1.1.1.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     2.2.2.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     3.3.3.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     4.4.4.0 255.255.255.0 [115/10] via 22.22.22.5, subint
i L2     5.5.5.0 255.255.255.0 [115/10] via 22.22.22.5, subint
```

show running-config

To display the configuration that is currently running on the ASA, use the **show running-config** command in privileged EXEC mode.

show running-config [**all**] [*command*]

Syntax Description

all	Displays the entire operating configuration, including defaults.
command	Displays the configuration associated with a specific command. For available commands, see the CLI help using **show running-config ?**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.3(1)	Encrypted passwords were added to the output.
9.7(1)	The output from this command will also display syslog servers configured with IPv6 addresses.
9.13(1)	• The telemetry configuration details were included in the output. • New command—**tftp blocksize** was added to display the configured blocksize value except the default value.

Usage Guidelines

The show running-config command displays the active configuration in memory (including saved configuration changes) on the ASA.

To display the saved configuration in flash memory on the ASA, use the **show configuration** command.

The **show running-config** command output displays encrypted, masked, or clear text passwords when password encryption is either enabled or disabled.

Note ASDM commands appear in the configuration after you use it to connect to or configure the ASA.

The default for **error-recovery disable** changed to disabled in ASA release 9.3. For that reason, you may notice that the **show running-config** command now shows *error-recovery disable* in the CLI when WebVPN error recovery is at the default value. We recommend to leave it disabled unless advised by Cisco's Technical Assistance Center while troubleshooting a problem.

From ASA 9.13(1), the telemetry details were included to the output of this command. The show running-config command shows only the non-default configuration (**no service telemetry**) of the telemetry service. Use the **all** command to also view the default telemetry service configuration.

Examples

The following is sample output from the **show running-config** command:

```
ciscoasa# show running-config
: Saved
:
ASA Version 9.0(1)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.1.1.2 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.3 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname example1
domain-name example.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
monitor-interface test
```

```
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.1.1.2
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map abc_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy abc_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

The following is sample output from the **show running-config access-group** command:

```
ciscoasa# show running-config access-group
access-group 100 in interface outside
```

The following is sample output from the **show running-config arp** command:

```
ciscoasa# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

To view the BFD global configuration settings, use output modifiers to filter the BFD related configuration. The following is sample output from the **show running-config bfd** command using the output modifiers:

```
ciscoasa# show running-config bfd
bfd map ipv4 1.1.1.1/24 1.1.1.2/32 name2
```

The following is sample output from the **show running-config bfd-template** command using the output modifiers:

```
ciscoasa# show running-config bfd-template
bfd-template single-hop bfd_template
interval min-tx 50 min-rx 50 multiplier 3
!
bfd-template single-hop bfd_template_auth
interval min-tx 50 min-rx 50 multiplier 3
authentication md5 ***** key-id 8
!
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
show configuration	Shows the startup configuration.

show s

show saml metadata

Show the SAML metadata tunnel-group-name.

show saml metadata tunnel-group-name

Syntax Description

Enter the name of the tunnel group to display SAML metadata for.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

Show SAML SP's metadata for a particular tunnel group.

Examples

The following is sample output from the **show scansafe server** command:

```
ciscoasa# show saml metadata saml_sso_tunnel_group
```

Related Commands

Command	Description
saml idp	Creates an inspection class map for whitelisted users and groups.

show scansafe server

To show the status of the Cloud Web Security proxy servers, use the **show scansafe server** command in privileged EXEC mode.

show scansafe server

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

This command shows the status of the server, whether it is the current active server, the backup server, or unreachable.

In multiple context mode, the output of this command depends on the admin-contexts ability to reach the Scansafe servers. The admin context makes regular poll attempts to verify whether the Scansafe server is up when no traffic is going through the ASA. The polling attempt interval is unconfigurable and is fixed at 15 minutes. The admin-context also sends keepalives to the Scansafe tower.

Examples

The following is sample output from the **show scansafe server** command:

```
ciscoasa# show scansafe server
ciscoasa# Primary: proxy197.scansafe.net (72.37.244.115) (REACHABLE)*
ciscoasa# Backup: proxy137.scansafe.net (80.254.152.99)
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.

Command	Description
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

show scansafe statistics

To show information about Cloud Web Security activity, use the **show scansafe statistics** command in privileged EXEC mode.

show scansafe statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

The **show scansafe statistics** command shows information about Cloud Web Security activity, such as the number of connections redirected to the proxy server, the number of current connections being redirected, and the number of whitelisted connections.

Examples

The following is sample output from the **show scansafe statistics** command:

```
ciscoasa# show scansafe statistics
Current HTTP sessions : 0
Current HTTPS sessions : 0
Total HTTP Sessions : 0
Total HTTPS Sessions : 0
Total Fail HTTP sessions : 0
Total Fail HTTPS sessions : 0
Total Bytes In : 0 Bytes
Total Bytes Out : 0 Bytes
HTTP session Connect Latency in ms(min/max/avg) : 0/0/0
HTTPS session Connect Latency in ms(min/max/avg) : 0/0/0
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.

Command	Description
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it’s the current active server, the backup server, or unreachable.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

show sctp

To display current Stream Control Transmission Protocol (SCTP) cookies and associations, use the **show sctp** command in privileged EXEC mode.

show sctp [**detail**]

Syntax Description

detail	Displays detailed information about SCTP associations.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.5(2)	This command was added.
9.7(1)	Detailed output now includes information about multi-homing, multiple streams, and frame reassembly.

Usage Guidelines

The **show sctp** command displays information about SCTP cookies and associations.

Examples

The following is sample output from the **show sctp** command:

```
ciscoasa# show sctp

AssocID: 2279da7a
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40174 (ESTABLISHED)
AssocID: 4924f520
Local:  192.168.107.11/20001 (ESTABLISHED)
Remote: 192.168.108.11/40200 (ESTABLISHED)
```

The following is sample output from the **show sctp detail** command:

```
ciscoasa(config)# show sctp detail


AssocID: 8b7e3ffb
Local:  192.168.100.56/3868 (ESTABLISHED)
    Receiver Window: 48000
    Cumulative TSN: 5cb6cd9b
    Next TSN: 5cb6cd9c
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
Remote: 192.168.200.78/3868 (ESTABLISHED)
    Receiver Window: 114688
    Cumulative TSN: 5cb6cd98
    Next TSN: 0
    Earliest Outstanding TSN: 5cb6cd9c
    Out-of-Order Packet Count: 0
```

Starting with 9.7(1), detailed output includes information about multi-homing, multiple streams, and frame reassembly.

```
asa2005# show sctp detail

AssocID: 2e590263
Local:  10.0.103.250/50000 (ESTABLISHED)
    Multi-homing IP's: 10.0.103.251(10.0.103.251)
    Receiver Window: 106496
    Cumulative TSN: bf0a3180
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
    Stream ID 3: next SN 10, first/last queued SN 11/16, hole SN:
    Stream ID 4: next SN 10, first/last queued SN 11/16, hole SN:
Remote: 10.0.102.250/3868 (CLOSED)
    Multi-homing IP's: 10.0.102.251(10.0.102.251)
    Receiver Window: 106496
    Cumulative TSN: 915d5916
    Next TSN: 0
    Earliest Outstanding TSN: 0
    Re-ordering queue:
Secondary Conn List:
    10.0.102.251(10.0.102.251):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.251(10.0.102.251):3868
    10.0.102.250(10.0.102.250):3868 to 10.0.103.251(10.0.103.251):50000
    10.0.103.251(10.0.103.251):50000 to 10.0.102.250(10.0.102.250):3868
    10.0.102.251(10.0.102.251):3868 to 10.0.103.250(10.0.103.250):50000
    10.0.103.250(10.0.103.250):50000 to 10.0.102.251(10.0.102.251):3868
```

Related Commands

Command	Description
show local-host	Shows information on hosts making connections through the ASA, per interface.
show service-policy inspect sctp	Shows SCTP inspection statistics.
show traffic	Shows connection and inspection statistics per interface

show service-policy

To display the service policy statistics, use the **show service-policy** command in privileged EXEC mode.

show service-policy [**global | interface** *intf*] [**csc | cxsc | inspect** *inspection* [*arguments*] **| ips | police | priority | set connection** [**details**] **| sfr | shape | user-statistics**]
show service-policy [**global | interface** *intf*] [**flow** *protocol* { **host** *src_host* | *src_ip src_mask* } [**eq** *src_port*] { **host** *dest_host* | *dest_ip dest_mask* } [**eq** *dest_port*] [*icmp_number* | *icmp_control_message*]]

Syntax Description

csc	(Optional) Shows detailed information about policies that include the **csc** command.
cxsc	(Optional) Shows detailed information about policies that include the **cxsc** command.
dest_ip dest_mask	For the **flow** keyword, the destination IP address and netmask of the traffic flow.
details	(Optional) For the **set connection** keyword, displays per-client connection information, if a per-client connection limit is enabled.
eq *dest_port*	(Optional) For the **flow** keyword, equals the destination port for the flow.
eq *src_port*	(Optional) For the **flow** keyword, equals the source port for the flow.
flow *protocol*	(Optional) Shows policies that match a particular flow identified by the 5-tuple (protocol, source IP address, source port, destination IP address, destination port). You can use this command to check that your service policy configuration will provide the services you want for specific connections. Because the flow is described as a 5-tuple, not all policies are supported. See the following supported policy matches: • **match access-list** • **match port** • **match rtp** • **match default-inspection-traffic**
global	(Optional) Limits output to the global policy.
host *dest_host*	For the **flow** keyword, the host destination IP address of the traffic flow.
host *src_host*	For the **flow** keyword, the host source IP address of the traffic flow.
icmp_control_message	(Optional) For the **flow** keyword when you specify ICMP as the protocol, specifies an ICMP control message of the traffic flow.
icmp_number	(Optional) For the **flow** keyword when you specify ICMP as the protocol, specifies the ICMP protocol number of the traffic flow.

inspect *inspection* [*arguments*]	(Optional) Shows detailed information about policies that include an **inspect** command. Not all **inspect** commands are supported for detailed output. To see all inspections, use the **show service-policy** command without any arguments. The arguments available for each inspection vary; see the CLI help for more information.
interface *intf*	(Optional) Displays policies applied to the interface specified by the *intf* argument, where *intf* is the interface name given by the **nameif** command.
ips	(Optional) Shows detailed information about policies that include the **ips** command.
police	(Optional) Shows detailed information about policies that include the **police** command.
priority	(Optional) Shows detailed information about policies that include the **priority** command.
set connection	(Optional) Shows detailed information about policies that include the **set connection** command.
sfr	(Optional) Shows detailed information about policies that include the **sfr** command.
shape	(Optional) Shows detailed information about policies that include the **shape** command.
src_ip src_mask	For the **flow** keyword, the source IP address and netmask used in the traffic flow.
user-statistics	(Optional) Shows detailed information about policies that include the **user-statistics** command. This command displays user statistics for the Identify Firewall, including sent packet count, sent drop count, received packet count, and send drop count for selected users.

Command Default

If you do not specify any arguments, this command shows all global and interface policies.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The **csc** keyword was added.

Release	Modification
7.2(4)/8.0(4)	The **shape** keyword was added.
8.4(2)	Support for the **user-statistics** keyword for the Identity Firewall was added.
8.4(4.1)	Support for the **cxsc** keyword for the ASA CX module was added.
9.2(1)	Support for the **sfr** keyword for the ASA FirePOWER module was added.
9.5(2)	The **inspect sctp** and **inspect diameter** keywords were added.
9.6(2)	The **inspect stun** and **inspect m3ua** { **drops** | **endpoint** *ip_address* } keywords were added.
9.7(1)	The **inspect m3ua session** and **inspect gtp pdpmcb teid** *teid* keywords were added. In addition, the limitation for showing rules was increased from 64 per class map to 128.
9.10(1)	The **detail** keyword was added to inspect dns. The detailed information provides more information about Cisco Umbrella.

Usage Guidelines

The number of embryonic connections displayed in the **show service-policy** command output indicates the current number of embryonic connections to an interface for traffic matching that defined by the **class-map** command. The "embryonic-conn-max" field shows the maximum embryonic limit configured for the traffic class using the Modular Policy Framework. If the current embryonic connections displayed equals or exceeds the maximum, TCP intercept is applied to new TCP connections that match the traffic type defined by the **class-map** command.

When you make service policy changes to the configuration, all *new* connections use the new service policy. Existing connections continue to use the policy that was configured at the time of the connection establishment. **show** command output will not include data about the old connections. For example, if you remove a QoS service policy from an interface, then re-add a modified version, then the **show service-policy** command only displays QoS counters associated with new connections that match the new service policy; existing connections on the old policy no longer show in the command output. To ensure that all connections use the new policy, you need to disconnect the current connections so they can reconnect using the new policy. See the **clear conn** or **clear local-host** commands.

Note For an **inspect icmp** and **inspect icmp error** policies, the packet counts only include the echo request and reply packets.

Examples

The following is sample output from the **show service-policy global** command:

```
ciscoasa# show service-policy global
Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
```

The following is sample output from the **show service-policy priority** command:

```
ciscoasa# show service-policy priority
```

```
Interface outside:
Global policy:
  Service-policy: sa_global_fw_policy
Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap
```

The following is sample output from the **show service-policy flow** command:

```
ciscoasa# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060
Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip
Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
       Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158 255.255.255.224

      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

The following is sample output from the **show service-policy inspect http** command. This example shows the statistics of each match command in a match-any class map.

```
ciscoasa# show service-policy inspect http
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: http http, packet 1916, drop 0, reset-drop 0
        protocol violations
          packet 0
        class http_any (match-any)
          Match: request method get, 638 packets
          Match: request method put, 10 packets
          Match: request method post, 0 packets
          Match: request method connect, 0 packets
          log, packet 648
```

For devices that have multiple CPU cores, there is a counter for lock failure. The locking mechanism is used to protect shared data structures and variables, because they can be used by multiple cores.When the core fails to acquire a lock, it tries to get the lock again. The lock fail counter increments for each failed attempt.

```
ciscoasa# show service-policy
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      ...
      Inspect: esmtp _default_esmtp_map, packet 96716502, lock fail 7, drop 25,
reset-drop 0
      Inspect: sqlnet, packet 2526511491, lock fail 21, drop 2362, reset-drop 0
```

The following is sample output from the **show service-policy inspect waas** command. This example shows the waas statistics.

```
ciscoasa# show service-policy inspect waas
Global policy:
  Service-policy: global_policy
    Class-map: WAAS
      Inspect: waas, packet 12, drop 0, reset-drop 0
  SYN with WAAS option 4
  SYN-ACK with WAAS option 4
  Confirmed WAAS connections 4
  Invalid ACKs seen on WAAS connections 0
  Data exceeding window size on WAAS connections 0
```

The following command shows the statistics for GTP inspection. The output is explained in Table 12-1.

```
firewall(config)# show service-policy inspect gtp statistics

GPRS GTP Statistics:
  version_not_support              0     msg_too_short             0
  unknown_msg                      0     unexpected_sig_msg        0
  unexpected_data_msg              0     ie_duplicated             0
  mandatory_ie_missing             0     mandatory_ie_incorrect    0
  optional_ie_incorrect            0     ie_unknown                0
  ie_out_of_order                  0     ie_unexpected             0
  total_forwarded                 67     total_dropped             1
  signalling_msg_dropped           1     data_msg_dropped          0
  signalling_msg_forwarded        67     data_msg_forwarded        0
  total created_pdp               33     total deleted_pdp         32
  total created_pdpmcb            31     total deleted_pdpmcb      30
  total dup_sig_mcbinfo            0     total dup_data_mcbinfo    0
  no_new_sgw_sig_mcbinfo           0     no_new_sgw_data_mcbinfo   0
  pdp_non_existent                 1
```

Table 81: GPRS GTP Statistics

Column Heading	Description
version_not_support	Displays packets with an unsupported GTP version field.
msg_too_short	Displays packets less than 8 bytes in length.
unknown_msg	Displays unknown type messages.
unexpected_sig_msg	Displays unexpected signaling messages.
unexpected_data_msg	Displays unexpected data messages.
mandatory_ie_missing	Displays messages missing a mandatory Information Element (IE).
mandatory_ie_incorrect	Displays messages with an incorrectly formatted mandatory Information Element (IE).
optional_ie_incorrect	Displays messages with an invalid optional Information Element (IE).
ie_unknown	Displays messages with an unknown Information Element (IE).

Column Heading	Description
ie_out_of_order	Displays messages with out-of-sequence Information Elements (IEs).
ie_unexpected	Displays messages with an unexpected Information Element (IE).
ie_duplicated	Displays messages with a duplicated Information Element (IE).
optional_ie_incorrect	Displays messages with an incorrectly formatted optional Information Element (IE).
total_dropped	Displays the total messages dropped.
signalling_msg_dropped	Displays the signaling messages dropped.
data_msg_dropped	Displays the data messages dropped.
total_forwarded	Displays the total messages forwarded.
signalling_msg_forwarded	Displays the signaling messages forwarded.
data_msg_forwarded	Displays the data messages forwarded.
total created_pdp	Displays the total Packet Data Protocol (PDP) or bearer contexts created.
total deleted_pdp	Displays the total Packet Data Protocol (PDP) or bearer contexts deleted.
total created_pdpmcb total deleted_pdpmcb total dup_sig_mcbinfo total dup_data_mcbinfo no_new_sgw_sig_mcbinfo no_new_sgw_data_mcbinfo	These fields relate to the use of PDP master control blocks, which is an implementation feature. These counters are used by Cisco Technical Support for troubleshooting and are not of direct interest to end users.
pdp_non_existent	Displays the messages received for a non-existent PDP context.

Examples

The following command displays information about the PDP contexts:

```
ciscoasa# show service-policy inspect gtp pdp-context
1 in use, 32 most used
Version TID                  MS Addr         SGSN Addr     Idle      Timeout   APN
v2      2692026893437055 10.0.0.1        10.0.0.11       0:00:11  0:04:00  gprs.example.com
```

Starting with ASA 9.6.2, GTP PDP context information is shown one per line instead of in a table. This makes it easier to read when using IPv6 addresses.

```
ciscoasa# show service-policy inspect gtp pdp-context
4 in use, 5 most used
Version v1,   TID 050542012151705f,  MS Addr 2005:a00::250:56ff:fe96:eec,
SGSN Addr 10.0.203.22,      Idle 0:52:01,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517056,  MS Addr 100.100.100.102,
SGW Addr 10.0.203.24,      Idle 0:00:05,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517057,  MS Addr 100.100.100.103,
SGW Addr 10.0.203.25,      Idle 0:00:04,   Timeout 3:00:00,   APN ssenoauth146
Version v2,   TID 0505420121517055,  MS Addr 100.100.100.101,
SGW Addr 10.0.203.23,      Idle 0:00:06,   Timeout 3:00:00,   APN ssenoauth146
```

Table 12-2 describes the output from the **show service-policy inspect gtp pdp-context** command.

Table 82: PDP Contexts

Column Heading	Description
Version	Displays the version of GTP.
TID	Displays the tunnel identifier.
MS Addr	Displays the mobile station address.
SGSN Addr SGW Addr	Displays the serving gateway service node (SGSN) or serving gateway (SGW).
Idle	Displays the time for which the PDP or bearer context has not been in use.
APN	Displays the access point name.

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears all service policy configurations.
service-policy	Configures the service policy.
show running-config service-policy	Displays the service policies configured in the running configuration.

show shared license

To show shared license statistics, use the **show shared license** command in privileged EXEC mode. Optional keywords are available only for the licensing server.

show shared license [**detail | client** [*hostname*] **| backup**]

Syntax Description

backup	(Optional) Shows information about the backup server.
client	(Optional) Limits the display to participants.
detail	(Optional) Shows all statistics, including per participant.
hostname	(Optional) Limits the display to a particular participant.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

To clear the statistics, enter the **clear shared license** command.

Examples

The following is sample output from the **show shared license** command on the license participant:

```
ciscoasa# show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive
Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
Client ID           Usage   Hostname
  ASA0926K04D         0       5510-B
```

Table 12-3 describes the output from the **show shared license** command.

Table 83: show shared license Description

Field	Description
Primary License Server	The IP address of the primary server.
Version	The shared license version.
Status	If the command is issued on the backup server, "Active" means that this device has taken on the role as a Primary Shared Licensing server. "Inactive" means that the device is ready in standby mode, and the device is communicating with the primary server. If failover is configured on the primary licensing server, the backup server may become "Active" for a brief moment during a failover but should return to "Inactive" after communications have synced up again.
Shared license utilization	
SSLVPN	
Total for network	Displays the total number of shared sessions available.
Available	Displays the remaining shared sessions available.
Utilized	Displays the shared sessions obtained for the active license server.
This device	
Platform limit	Displays the total number of SSL VPN sessions for this device according to the installed license.
Current usage	Displays the number of shared SSL VPN session currently owned by this device from the shared pool.
High usage	Displays the highest number of shared SSL VPN sessions ever owned by this device.
Messages Tx/Rx/Error	
RegistrationGetReleaseTransfer	Shows the Transmit, Received, and Error packets of each type of connection.
Client ID	A unique client ID.
Usage	Displays the number of sessions in use.
Hostname	Displays the hostname for this device.

Examples

The following is sample output from the **show shared license detail** command on the license server:

```
ciscoasa# show shared license detail
Backup License Server Info:
Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0
Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
Client Info:
  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

Related Commands

Command	Description
activation-key	Enters a license activation key.
clear configure license-server	Clears the shared licensing server configuration.
clear shared license	Clears shared license statistics.
license-server address	Identifies the shared licensing server IP address and shared secret for a participant.
license-server backup address	Identifies the shared licensing backup server for a participant.
license-server backup backup-id	Identifies the backup server IP address and serial number for the main shared licensing server.
license-server backup enable	Enables a unit to be the shared licensing backup server.
license-server enable	Enables a unit to be the shared licensing server.

Command	Description
license-server port	Sets the port on which the server listens for SSL connections from participants.
license-server refresh-interval	Sets the refresh interval provided to participants to set how often they should communicate with the server.
license-server secret	Sets the shared secret on the shared licensing server.
show activation-key	Shows the current licenses installed.
show running-config license-server	Shows the shared licensing server configuration.
show vpn-sessiondb	Shows license information about VPN sessions.

show shun

To display shun information, use the **show shun** command in privileged EXEC mode.

show shun [*src_ip* | *statistics*]

Syntax Description

src_ip	(Optional) Displays the information for that address.
statistics	(Optional) Displays the interface counters only.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Examples

The following is sample output from the **show shun** command:

```
ciscoasa# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
shun	Enables a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection.

show sip

To display SIP sessions, use the show **sip** command in privileged EXEC mode.

show sip

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show sip** command displays information for SIP sessions established across the ASA.

Note We recommend that you configure the **pager** command before using the **show sip** command. If there are a lot of SIP session records and the **pager** command is not configured, it will take a while for the **show sip** command output to reach its end.

Examples

The following is sample output from the **show sip** command:

```
ciscoasa# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

This sample shows two active SIP sessions on the ASA (as shown in the Total field). Each call-id represents a call.

The first session, with the call-id c3943000-960ca-2e43-228f@10.130.56.44, is in the state Call Init , which means the session is still in call setup. Call setup is complete only when the ACK is seen. This session has been idle for 1 second.

The second session is in the state Active , in which call setup is complete and the endpoints are exchanging media. This session has been idle for 6 seconds.

Related Commands

Commands	Description
inspect sip	Enables SIP application inspection.
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show skinny

To troubleshoot SCCP (Skinny) inspection engine issues, use the show skinny command in privileged EXEC mode.

show skinny

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show skinny** command displays information for SCCP (Skinny) sessions.

Examples

The following is sample output from the **show skinny** command under the following conditions. There are two active Skinny sessions set up across the ASA. The first one is established between an internal Cisco IP Phone at local address 10.0.0.11 and an external Cisco CallManager at 172.18.1.33. TCP port 2000 is the CallManager. The second one is established between another internal Cisco IP Phone at local address 10.0.0.22 and the same Cisco CallManager.

```
ciscoasa# show skinny
MEDIA 10.0.0.22/20798         172.18.1.11/22948
LOCAL                   FOREIGN                STATE
---------------------------------------------------------------
1       10.0.0.11/52238         172.18.1.33/2000               1
  MEDIA 10.0.0.11/22948         172.18.1.22/20798
2       10.0.0.22/52232         172.18.1.33/2000               1
  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

The output indicates a call has been established between both internal Cisco IP Phones. The RTP listening ports of the first and second phones are UDP 22948 and 20798 respectively.

Related Commands

Commands	Description
inspect skinny	Enables SCCP application inspection.

Commands	Description
show conn	Displays the connection state for different connection types.
timeout	Sets the maximum idle time duration for different protocols and session types.

show sla monitor configuration

To display the configuration values, including the defaults, for SLA operations, use the **show sla monitor configuration** command in user EXEC mode.

show sla monitor configuration [*sla-id*]

Syntax Description

sla-id	(Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Command Default

If the *sla-id* is not specified, the configuration values for all SLA operations are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use the **show running config sla monitor** command to see the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor** command. It displays the configuration values for SLA operation 123. Following the output of the **show sla monitor** command is the output of the **show running-config sla monitor** command for the same SLA operation.

```
ciscoasa> show sla monitor 124
SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
```

```
Status of entry (SNMP RowStatus): Active
Enhanced History:
ciscoasa# show running-config sla monitor 124
sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.
sla monitor	Defines an SLA monitoring operation.

show sla monitor operational-state

To display the operational state of SLA operations, use the **show sla monitor operational-state** command in user EXEC mode.

show sla monitor operational-state [*sla-id*]

Syntax Description

sla-id	(Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.

Command Default

If the *sla-id* is not specified, statistics for all SLA operations are displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

Use the **show running-config sla monitor** command to display the SLA operation commands in the running configuration.

Examples

The following is sample output from the **show sla monitor operational-state** command:

```
ciscoasa> show sla monitor operationl-state
Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

Related Commands

Command	Description
show running-config sla monitor	Displays the SLA operation configuration commands in the running configuration.
sla monitor	Defines an SLA monitoring operation.

show snmp-server engineid

To display the identification of the SNMP engine that has been configured on the ASA, use the **show snmp-server engineid** command in privileged EXEC mode.

show snmp-server engineid

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following is sample output from the **show snmp-server engineid** command:

```
ciscoasa
#
show snmp-server engineid
Local SNMP engineID: 80000009fe85f8fd882920834a3af7e4ca79a0a1220fe10685
```

Usage Guidelines

An SNMP engine is a copy of SNMP that can reside on a local device. The engine ID is a unique value that is assigned for each SNMP agent for each ASA context. The engine ID is not configurable on the ASA. The engine ID is 25 bytes long, and is used to generate encrypted passwords. The encrypted passwords are then stored in flash memory. The engine ID can be cached. In a failover pair, the engine ID is synchronized with the peer.

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server group

To display the names of configured SNMP groups, the security model being used, the status of different views, and the storage type of each group, use the **show snmp-server group** command in privileged EXEC mode.

show snmp-server group

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following is sample output from the **show snmp-server group** command:

```
ciscoasa
#
show snmp-server group
groupname: public                          security model:v1
readview : <no readview specified>         writeview: <no writeview specified>
notifyview: <no readview specified>
row status: active
groupname: public                          security model:v2c
readview : <no readview specified>         writeview: <no writeview specified>
notifyview: *<no readview specified>
row status: active
groupname: privgroup                  security model:v3 priv
readview : def_read_view              writeview: <no writeview specified>
notifyview: def_notify_view
row status: active
```

Usage Guidelines

SNMP users and groups are used according to the View-based Access Control Model (VACM) for SNMP. The SNMP group determines the security model to be used. The SNMP user should match the security model of the SNMP group. Each SNMP group name and security level pair must be unique.

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.

Command	Description
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server host

To display the names of configured SNMP hosts that belong to a host group, the interface being used, and the version of SNMP being used, use the **show snmp-server host** command in privileged EXEC mode.

show snmp-server host

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
9.4(1)	The output was updated to show only active hosts that are polling the ASA, as well as the statically configured hosts.

Examples

The following is sample output from the **show snmp-server host** command:

```
ciscoasa
#
show snmp-server host
host ip = 10.10.10.1, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.10, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.2, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.4, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.5, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.7, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.8, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.9, interface = mgmt  poll community ***** version 2c
```

The following is sample output from the **show snmp-server host** command as of Version 9.4(1), which shows only the active hosts polling the ASA:

```
ciscoasa
#
show snmp-server host
```

```
host ip = 10.10.10.3, interface = mgmt  poll community ***** version 2c
host ip = 10.10.10.6, interface = mgmt  poll community ***** version 2c
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server statistics

To display SNMP server statistics, use the **show snmp-server statistics** command in privileged EXEC mode.

show snmp-server statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following is sample output from the **show snmp-server statistics** command:

```
ciscoasa# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
clear snmp-server statistics	Clears the SNMP packet input and output counters.

Command	Description
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show snmp-server user

To display information about the configured characteristics of SNMP users, use the **show snmp-server user** command in privileged EXEC mode.

show snmp-server user [*username*]

Syntax Description

username	(Optional) Identifies a specific user or users about which to display SNMP information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.

Examples

The following is sample output from the **show snmp-server user** command:

```
ciscoasa
#
show snmp-server user authuser
User name: authuser
Engine ID: 00000009020000000C025808
storage-type: nonvolatile       active access-list: N/A
Rowstatus: active
Authentication Protocol: MD5
Privacy protocol: DES
Group name: VacmGroupName
```

The output provides the following information:

- The username, which is a string that identifies the name of the SNMP user.
- The engine ID, which is a string that identifies the copy of SNMP on the ASA.
- The storage-type, which indicates whether or not the settings have been set in volatile or temporary memory on the ASA, or in nonvolatile or persistent memory, in which settings remain after the ASA has been turned off and on again.
- The active access list, which is the standard IP access list associated with the SNMP user.
- The Rowstatus, which indicates whether or not it is active or inactive.

- The authentication protocol, which identifies which authentication protocol is being used. Options are MD5, SHA, or none. If authentication is not supported in your software image, this field does not appear.
- The privacy protocol, which indicates whether or not DES packet encryption is enabled. If privacy is not supported in your software image, this field does not appear.
- The group name, which indicates to which SNMP group the user belongs. SNMP groups are defined according to the View-based Access Control Model (VACM).

Usage Guidelines

An SNMP user must be part of an SNMP group. If you do not enter the *username* argument, the **show snmp-server user** command displays information about all configured users. If you enter the *username* argument and the user exists, the information about that user appears.

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
show running-config snmp-server	Displays the SNMP server configuration.
snmp-server	Configures the SNMP server.

show software authenticity development

To verify that the loading of development key signed images is enabled or disabled, use the **show software authenticity development** command in privileged EXEC mode.

show software authenticity development

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity file** command:

```
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

Related Commands

Command	Description
show version	Displays the software version, hardware configuration, license key, and related uptime data.
software authenticity key add special	Adds a new development key to SPI flash.
software authenticity key revoke special	Deletes older development keys from SPI flash.
show software authenticity keys	Displays the development keys in SPI flash.
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the development keys file.
show software authenticity running	Displays the digital signature information related to the current running file.

Command	Description
show software authenticity	Displays digital signature information related to software authentication for a specific image file.

show software authenticity file

To display digital signature information related to software authentication for a specific image file, use the **show software authenticity file** command in privileged EXEC mode.

show software authenticity [*filename*]

Syntax Description

filename	(Optional) Identifies a specific image file.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity file** command:

```
ciscoasa
#
show software authenticity file asa913.SSA
File Name                     : disk0:/asa913.SSA
Image type                    : Development
    Signer Information
        Common Name           : Cisco
        Organization Unit     : ASA5585-X
        Organization Name     : Engineering
    Certificate Serial Number : abcd1234efgh5678
    Hash Algorithm            : SHA512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
```

The output provides the following information:

- The filename, which is the name of the filename in memory.
- The image type, which is the type of image being shown.
- The signer information specifies the signature information, which includes the following:
- The common name, which is the name of the software manufacturer.
- The organization unit, which indicates the hardware that the software image is deployed on.

- The organization name, which is the owner of the software image.
- The certificate serial number, which is the certificate serial number for the digital signature.
- The hash algorithm, which indicates the type of hash algorithm used in digital signature verification.
- The signature algorithm, which identifies the type of signature algorithm used in digital signature verification.
- The key version, which indicates the key version used for verification.

Related Commands

Command	Description
show version	Displays the software version, hardware configuration, license key, and related uptime data.

show software authenticity keys

To display information about development keys and release keys that are stored in SPI flash, use the **show software authenticity keys** command in privileged EXEC mode.

show software authenticity keys

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity keys** command:

```
ciscoasa# show software authenticity keys
Public Key #1 Information
--------------------------
Key Type              : Development (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
Public Key #2 Information
--------------------------
```

```
Key Type              : Release (Primary)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        96:A2:E6:E4:51:4D:4A:B0:F0:EF:DB:41:82:A6:AC:D0:
        FC:11:40:C2:F0:76:10:19:CE:D0:16:7D:26:73:B1:55:
        FE:42:FE:5D:5F:4D:A5:D5:29:7F:91:EC:91:4D:9B:33:
        54:4B:B8:4D:85:E9:11:2D:79:19:AA:C5:E7:2C:22:5E:
        F6:66:27:98:1C:5A:84:5E:25:E7:B9:09:80:C7:CD:F4:
        13:FB:32:6B:25:B5:22:DE:CD:DC:BE:65:D5:6A:99:02:
        95:89:78:8D:1A:39:A3:14:C9:32:EE:02:4C:AB:25:D0:
        38:AD:E4:C9:C6:6B:28:FE:93:C3:0A:FE:90:D4:22:CC:
        FF:99:62:25:57:FB:A7:C6:E4:A5:B2:22:C7:35:91:F8:
        BB:2A:19:42:85:8F:5E:2E:BF:A0:9D:57:94:DF:29:45:
        AA:31:56:6B:7C:C4:5B:54:FE:DE:30:31:B4:FC:4E:0C:
        9D:D8:16:DB:1D:3D:8A:98:6A:BB:C2:34:8B:B4:AA:D1:
        53:66:FF:89:FB:C2:13:12:7D:5B:60:16:CA:D8:17:54:
        7B:41:1D:31:EF:54:DB:49:40:1F:99:FB:18:38:03:EE:
        2D:E8:E1:9F:E6:B2:C3:1C:55:70:F4:F3:B2:E7:4A:5A:
        F5:AA:1D:03:BD:A1:C3:9F:97:80:E6:63:05:27:F2:1F
Exponent              : 65537
Key Version           : A
Public Key #3 Information
-------------------------
Key Type              : Development (Backup)
Public Key Algorithm  : 2048-bit RSA
Modulus :
        E1:61:22:18:6D:0D:A3:D8:C8:54:62:0D:8D:9A:0E:09:
        05:C8:02:5C:B6:51:47:C7:23:AF:1D:1E:AC:8D:9D:0E:
        DD:30:3C:50:26:F6:E8:26:F9:D7:69:D2:1E:DA:4E:24:
        99:D4:A5:A6:13:68:8D:B0:53:39:02:61:64:81:70:94:
        27:A3:31:A5:05:95:63:AF:EA:EB:26:AB:39:8C:31:6A:
        DD:13:22:22:41:A7:3A:FC:19:80:BE:FC:13:2A:C1:39:
        E0:E6:70:1B:DE:4F:69:EB:92:84:34:23:61:AE:46:53:
        C4:68:4E:DE:A3:98:F6:2E:5A:B5:AC:18:05:90:37:80:
        7C:3E:08:E3:03:83:91:30:11:29:E3:12:B0:26:23:AC:
        0A:C0:DE:31:9D:4B:14:D8:A6:78:B8:B5:84:04:EA:C7:
        FB:CF:C1:DD:16:75:82:FC:1B:5C:FF:B7:C0:36:88:E3:
        3E:BE:44:82:65:2F:66:FF:25:1A:FA:2C:B2:03:17:16:
        0D:C8:33:4F:13:C6:62:D8:53:FC:11:1A:9C:3C:10:EE:
        09:32:FE:38:C2:A2:E2:56:E5:ED:93:89:40:46:B9:E4:
        B3:9C:68:76:B0:BF:0D:FD:33:E6:F6:8C:26:D9:FF:F9:
        DA:B5:D4:86:81:B4:D1:3B:5E:81:1E:20:9F:BE:6E:B7
Exponent              : 65537
Key Version           : A
```

Related Commands

Command	Description
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the Development Key file.
show software authenticity keys	Displays the Development Keys.
show software authenticity running	Displays the digital signature information related to the current running file.
software authenticity key add special	Adds a new Development Key to SPR flash.
software authenticity key revoke special	Deletes older Development Keys from SPR flash.

show software authenticity running

To display digital signature information related to software authentication for a specific image file, use the **show software authenticity running** command in privileged EXEC mode. This command is the same as **show software authenticity file** except that it displays the digital signature information related to the current running file.

show software authenticity running

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following is sample output from the **show software authenticity running** command:

```
ciscoasa# show software authenticity running
Image type                    : Development
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 5448091A
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
    Verifier Information
        Verifier Name         : ROMMON
        Verifier Version      : Cisco Systems ROMMON,1.0.16
```

The output provides the following information:

- The filename, which is the name of the filename in memory.
- The image type, which is the type of image being shown.
- The signer information specifies the signature information, which includes the following:
- The common name, which is the name of the software manufacturer.

- The organization unit, which indicates the hardware that the software image is deployed on.
- The organization name, which is the owner of the software image.
- The certificate serial number, which is the certificate serial number for the digital signature.
- The hash algorithm, which indicates the type of hash algorithm used in digital signature verification.
- The signature algorithm, which identifies the type of signature algorithm used in digital signature verification.
- The key version, which indicates the key version used for verification.

Related Commands

Command	Description
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the Development Key file.
software authenticity key add special	Adds a new Development Key to SPR flash.
software authenticity key revoke special	Deletes older Development Keys from SPR flash.

show ssd

To view the status of the SSDs, use the **show ssd** command.

Note This command is only supported on the Secure Firewall 3100.

show ssd

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.17(1)	This command was introduced.

Examples

The following sample display shows information about the SSDs:

```
> show ssd
Local Disk: 1
Name: nvme0n1
Size(MB): 858306
Operability:
operable
Presence:
equipped
Model: Micron_7300_MTFDHBE960TDF
Serial: MSA244302N0
Drive State: online
SED Support:
yes
SED State:
unlocked
SED Auth Status: ok
RAID action: none
```

Related Commands

Command	Description
raid	Adds or removes an SSD from the RAID.
show raid	Shows the RAID status.

show ssh sessions

To display information about the active SSH sessions on the ASA, use the **show ssh sessions** command in privileged EXEC mode.

show ssh sessions [**hostname** *or* **A.B.C.D**] [**hostname** *or* **X:X:X:X::X**] [**detail**]

Syntax Description

hostname or **A.B.C.D**	(Optional) Displays SSH session information for only the specified SSH client IPv4 address.
hostname or **X:X:X:X::X**	(Optional) Displays SSH session information for only the specified SSH client IPv6 address.
detail	Displays detailed SSH session information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.1(2)	The **detail** option was added.

Usage Guidelines

The SID is a unique number that identifies the SSH session. The Client IP is the IP address of the system running an SSH client. The Version is the protocol version number that the SSH client supports. If the SSH only supports SSH version 1, then the Version column displays 1.5. If the SSH client supports both SSH version 1 and SSH version 2, then the Version column displays 1.99. If the SSH client only supports SSH version 2, then the Version column displays 2.0. The Encryption column shows the type of encryption that the SSH client is using. The State column shows the progress that the client is making as it interacts with the ASA. The Username column lists the login username that has been authenticated for the session. The Mode column describes the direction of the SSH data streams.

For SSH version 2, which can use the same or different encryption algorithms, the Mode field displays in and out. For SSH version 1, which uses the same encryption in both directions, the Mode field displays nil ('-') and allows only one entry per connection.

Examples

The following is sample output from the **show ssh sessions** command:

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

The following is sample output from the **show ssh sessions detail** command:

```
ciscoasa# show ssh sessions detail
SSH Session ID            : 0
>   Client IP             : 161.44.66.200
>   Username              : root
>   SSH Version           : 2.0
>   State                 : SessionStarted
>   Inbound Statistics
>    Encryption           : aes256-cbc
>    HMAC                 : sha1
>    Bytes Received       : 2224
>   Outbound Statistics
>    Encryption           : aes256-cbc
>    HMAC                 : sha1
>    Bytes Transmitted    : 2856
>   Rekey Information
>    Time Remaining (sec)  : 3297
>    Data Remaining (bytes): 996145356
>    Last Rekey           : 16:17:19.732 EST Wed Jan 2 2013
>    Data-Based Rekeys    : 0
>    Time-Based Rekeys    : 0
```

Related Commands

Command	Description
ssh disconnect	Disconnects an active SSH session.
ssh timeout	Sets the timeout value for idle SSH sessions.

show ssl

To display information about the SSL configuration and active SSL sessions on the ASA, use the **show ssl** command in privileged EXEC mode.

show ssl [**cache | ciphers** [*level*] | **errors | information | mib | objects**]

Syntax Description

cache	(Optional) Displays SSL session cache statistics.
ciphers [*level*]	(Optional) Displays which ciphers are configured for use, based on the levels that are configured using the **ssl cipher** command. You can specify one of the following levels to see just the ciphers at that level. If you do not specify a level, the medium level for each SSL/TLS/DTLS version are shown. • **all** —Includes all ciphers. • **low** —Includes all ciphers except NULL-SHA. • **medium** —Includes all ciphers except the null, DES, and RC4 ciphers. • **fips** —Includes all FIPS-compliant ciphers. • **high** —Applies only to TLSv1.2, and includes only the strongest ciphers.
errors	(Optional) Displays SSL errors.
information	(Optional) Displays SSL supported configuration either with or without 3DES license and all ciphers that can be supported on the device.
mib	(Optional) Displays SSL MIB statistics.
objects	(Optional) Displays SSL object statistics.

Command Default

For show ssl information, the following default settings are applied with or without 3DES:

- Default setting without 3DES (or higher cipher support):

```
ssl server-version tlsv1 dtlsv1
ssl client-version tlsv1
ssl cipher default low
ssl cipher tlsv1 low
ssl cipher tlsv1.1 low
ssl cipher tlsv1.2 low
ssl cipher dtlsv1 low
ssl cipher dtlsv1.2 low
ssl dh-group group2
ssl ecdh-group group19
ssl certificate-authentication fca-timeout 2
```

- Default setting with 3DES (or higher cipher support):

```
ssl server-version tlsv1 dtlsv1
ssl client-version tlsv1 dtlsv1
ssl cipher default medium
ssl cipher tlsv1 medium
ssl cipher tlsv1.1 medium
ssl cipher tlsv1.2 medium
ssl cipher dtlsv1 medium
ssl cipher dtlsv1.2 medium
ssl dh-group group2
ssl ecdh-group group19
ssl certificate-authentication fca-timeout 2
```

The following output is for the show ssl cache command

```
SSL session cache statistics:
  Maximum cache size:          750    Current cache size:          5
  Cache hits:                    0    Cache misses:                0
  Cache timeouts:                0    Cache full:                  0
  Accept attempts:               5    Accepts successful:          5
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:         0
  Connect renegotiates:          0
SSL VPNLB session cache statistics:
  Maximum cache size:           10    Current cache size:          0
  Cache hits:                    0    Cache misses:                0
  Cache timeouts:                0    Cache full:                  0
  Accept attempts:               0    Accepts successful:          0
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:         0
  Connect renegotiates:          0
DTLS session cache statistics:
  Maximum cache size:          750    Current cache size:          1
  Cache hits:                    1    Cache misses:                0
  Cache timeouts:                0    Cache full:                  0
  Accept attempts:               2    Accepts successful:          1
  Accept renegotiates:           0
  Connect attempts:              0    Connects successful:         0
  Connect renegotiates:          0
```

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.16(1)	Output of the `show ssl cache` command has been updated to remove SSLDEV session cache statistics.
9.12(1)	The show ssl cipher all command was removed and deprecated, and the show ssl cipher information command was added.
9.3(2)	Support for TLSv1.1 and TLSv1.2 was added. The **ciphers** keyword was added.
9.1(2)	The **detail** option was added.

Release	Modification
9.0(1)	Support for multiple context mode was added.
8.4(1)	This command was added.

Usage Guidelines

This command shows information about the current SSLv2 and SSLv3 sessions, including the enabled cipher order, which ciphers are disabled, SSL trustpoints being used, and whether or not certificate authentication is enabled.

Examples

The following is sample output from the **show ssl** command:

```
ciscoasa# show ssl
Accept connections using SSLv2 or greater and negotiate to TLSv1.2 or greater
Start connections using SSLv3 and negotiate to SSLv3 or greater
SSL DH Group: group2
SSL trust-points:
  Self-signed RSA certificate available
  Default: certsha256
  Interface inside: certsha256
Certificate authentication is not enabled
```

The following is sample output from the **show ssl ciphers fips** command:

```
ciscoasa# show ssl ciphers fips

  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
```

The following is output from the **show ssl ciphers** command.

```
ciscoasa# show ssl ciphers all

These are the ciphers for the given cipher level; not all ciphers
are supported by all versions of SSL/TLS.
These names can be used to create a custom cipher list
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (tlsv1)
  RC4-MD5 (tlsv1)
  DES-CBC-SHA (tlsv1)
  NULL-SHA (tlsv1)
asa3(config-tlsp)# show ssl ciphers medium
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers fips
  ECDHE-ECDSA-AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  DHE-RSA-AES256-GCM-SHA384 (tlsv1.2)
  AES256-GCM-SHA384 (tlsv1.2)
  ECDHE-ECDSA-AES256-SHA384 (tlsv1.2)
  ECDHE-RSA-AES256-SHA384 (tlsv1.2)
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  DHE-RSA-AES128-GCM-SHA256 (tlsv1.2)
  AES128-GCM-SHA256 (tlsv1.2)
  ECDHE-ECDSA-AES128-SHA256 (tlsv1.2)
  ECDHE-RSA-AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
asa3(config-tlsp)# show ssl ciphers
Current cipher configuration:
```

```
default (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
tlsv1.2 (medium):
  ECDHE-ECDSA-AES256-GCM-SHA384
  ECDHE-RSA-AES256-GCM-SHA384
  DHE-RSA-AES256-GCM-SHA384
  AES256-GCM-SHA384
  ECDHE-ECDSA-AES256-SHA384
  ECDHE-RSA-AES256-SHA384
  DHE-RSA-AES256-SHA256
  AES256-SHA256
  ECDHE-ECDSA-AES128-GCM-SHA256
  ECDHE-RSA-AES128-GCM-SHA256
  DHE-RSA-AES128-GCM-SHA256
  AES128-GCM-SHA256
  ECDHE-ECDSA-AES128-SHA256
  ECDHE-RSA-AES128-SHA256
  DHE-RSA-AES128-SHA256
  AES128-SHA256
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
dtlsv1 (medium):
  DHE-RSA-AES256-SHA
  AES256-SHA
  DHE-RSA-AES128-SHA
  AES128-SHA
```

Related Commands

Command	Description
license-server port	Sets the port on which the server listens for SSL connections from participants.

Command	Description
ssl ciphers	Specifies the encryption algorithms for the SSL, DTLS, and TLS protocols.

show startup-config

To show the startup configuration or to show any errors when the startup configuration loaded, use the **show startup-config** command in privileged EXEC mode.

show startup-config [**errors**]

Syntax Description

errors	(Optional) Shows any errors that were generated when the ASA loaded the startup configuration.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System[1]
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

[1]The errors keyword is only available in single mode and the system execution space.

Command History

Release	Modification
7.0(1)	The **errors** keyword was added.
8.3(1)	Encrypted passwords were added to the output.

Usage Guidelines

In multiple context mode, the **show startup-config** command shows the startup configuration for your current execution space: the system configuration or the security context.

The **show startup-config** command output displays encrypted, masked, or clear text passwords when password encryption is either enabled or disabled.

To clear the startup errors from memory, use the **clear startup-config errors** command.

Examples

The following is sample output from the **show startup-config** command:

```
ciscoasa# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003
Version 7.X(X)
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 209.165.200.224
 webvpn enable
!
interface GigabitEthernet0/1
```

```
 shutdown
 nameif test
 security-level 0
 ip address 209.165.200.225
!
...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 209.165.200.226
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!
...
Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

The following is sample output from the **show startup-config errors** command:

```
ciscoasa# show startup-config errors
ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', "nameif inside"
.....
*** Output from config line 37, "config-url disk:/admin..."
```

Related Commands

Command	Description
clear startup-config errors	Clears the startup errors from memory.
show running-config	Shows the running configuration.

show sunrpc-server active

To display the pinholes open for Sun RPC services, use the **show sunrpc-server active** command in privileged EXEC mode.

show sunrpc-server active

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **show sunrpc-server active** command to display the pinholes open for Sun RPC services, such as NFS and NIS.

Examples

To display the pinholes open for Sun RPC services, enter the **show sunrpc-server active** command. The following is sample output from the **show sunrpc-server active** command:

```
ciscoasa# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

The entry in the LOCAL column shows the IP address of the client or server on the inside interface, while the value in the FOREIGN column shows the IP address of the client or server on the outside interface.

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the ASA.
clear sunrpc-server active	Clears the pinholes opened for Sun RPC services, such as NFS or NIS.
inspect sunrpc	Enables or disables Sun RPC application inspection and configures the port used.
show running-config sunrpc-server	Displays information about the SunRPC services configuration.

show switch mac-address-table

To view the switch MAC address table, use the **show switch mac-address-table** command in privileged EXEC mode.

show switch mac-address-table

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

The switch MAC address table maintains the MAC address-to-switch port mapping for traffic within each VLAN in the switch hardware. If you are in transparent firewall mode, use the **show mac-address-table** command to view the bridge MAC address table in the ASA software. The bridge MAC address table maintains the MAC address-to-VLAN interface mapping for traffic that passes between VLANs.

MAC address entries age out in 5 minutes.

Examples

The following is sample output from the **show switch mac-address-table** command.

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
   Mac Address  | VLAN |       Type       | Age | Port
-------------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic      | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic      | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic      | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic      | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static       |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast |  -  | In0/1,Et0/0-7
Total Entries: 6
```

Table 12-4 shows each field description:

Table 84: show switch mac-address-table Fields

Field	Description
Mac Address	Shows the MAC address.
VLAN	Shows the VLAN associated with the MAC address.
Type	Shows if the MAC address was learned dynamically, as a static multicast address, or statically. The only static entry is for the internal backplane interface.
Age	Shows the age of a dynamic entry in the MAC address table.
Port	Shows the switch port through which the host with the MAC address can be reached.

Related Commands

Command	Description
show mac-address-table	Shows the MAC address table for models that do not have a built-in switch.
show switch vlan	Shows the VLAN and physical MAC address association.

show switch vlan

To view the VLANs and the associated switch ports, use the **show switch vlan** command in privileged EXEC mode.

show switch vlan

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

This command is for models with built-in switches only. For other models, use the **show vlan** command.

Examples

The following is sample output from the **show switch vlan** command.

```
ciscoasa# show switch vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------
100  inside                           up        Et0/0, Et0/1
200  outside                          up        Et0/7
300  -                                down      Et0/1, Et0/2
400  backup                           down      Et0/3
```

Table 12-4 shows each field description:

Table 85: show switch vlan Fields

Field	Description
VLAN	Shows the VLAN number.
Name	Shows the name of the VLAN interface. If no name is set using the **nameif** command, or if there is no **interface vlan** command, the display shows a dash (-).
Status	Shows the status, up or down, to receive and send traffic to and from the VLAN in the switch. At least one switch port in the VLAN needs to be in an up state for the VLAN state to be up.
Ports	Shows the switch ports assigned to each VLAN. If a switch port is listed for multiple VLANs, it is a trunk port. The above sample output shows Ethernet 0/1 is a trunk port that carries VLAN 100 and 300.

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show vlan	Shows the VLANs for models that do not have built-in switches.
switchport mode	Sets the mode of the switch port to access or trunk mode.

show sw-reset-button

To show whether the ASA 5506-X, 5508-X, or 5516-X software reset button is enabled, use the **show sw-reset-button** command in privileged EXEC mode.

show sw-reset-button

Syntax Description

This command has no arguments or keywords.

Command Default

The software reset button is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2))	Command added.

Usage Guidelines

Enable or disable the software reset button using the **service sw-reset-button** command. The reset button is a small recessed button on the rear panel that if pressed for longer than three seconds resets the ASA to its default “as-shipped” state following the next reboot. Configuration variables are reset to factory default. However, the flash is not erased, and no files are removed.

Examples

The following example enables the software reset button:

```
ciscoasa(config)# service sw-reset-button
ciscoasa(config)# show sw-reset-button
Software Reset Button is configured.
```

The following example disables the software reset button:

```
ciscoasa(config)# no service sw-reset-button
ciscoasa(config)# show sw-reset-button
Software Reset Button is not configured.
```

Related Commands

Command	Description
service sw-reset-button	Enables or disables the software reset button.

show t

show tcpstat

To display the status of the ASA TCP stack and the TCP connections that are terminated on the ASA (for debugging), use the **show tcpstat** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show tcpstat

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the ASA. The TCP statistics displayed are described in Table 28 .

Table 86: TCP Statistics in the show tcpstat Command

Statistic	Description
tcb_cnt	Number of TCP users.
proxy_cnt	Number of TCP proxies. TCP proxies are used by user authorization.
tcp_xmt pkts	Number of packets that were transmitted by the TCP stack.
tcp_rcv good pkts	Number of good packets that were received by the TCP stack.
tcp_rcv drop pkts	Number of received packets that the TCP stack dropped.
tcp bad chksum	Number of received packets that had a bad checksum.
tcp user hash add	Number of TCP users that were added to the hash table.
tcp user hash add dup	Number of times a TCP user was already in the hash table when trying to add a new user.

Statistic	Description
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.
tcp user srch hash miss	Number of times a TCP user was not found in the hash table when searching.
tcp user hash delete	Number of times that a TCP user was deleted from the hash table.
tcp user hash delete miss	Number of times that a TCP user was not found in the hash table when trying to delete the user.
lip	Local IP address of the TCP user.
fip	Foreign IP address of the TCP user.
lp	Local port of the TCP user.
fp	Foreign port of the TCP user.

st	State (see RFC 793) of the TCP user. The possible values are as follows:
	`1   CLOSED`
	`2   LISTEN`
	`3   SYN_SENT`
	`4   SYN_RCVD`
	`5   ESTABLISHED`
	`6   FIN_WAIT_1`
	`7   FIN_WAIT_2`
	`8   CLOSE_WAIT`
	`9   CLOSING`
	`10  LAST_ACK`
	`11  TIME_WAIT`

rexqlen	Length of the retransmit queue of the TCP user.
inqlen	Length of the input queue of the TCP user.
tw_timer	Value of the time_wait timer (in milliseconds) of the TCP user.
to_timer	Value of the inactivity timeout timer (in milliseconds) of the TCP user.
cl_timer	Value of the close request timer (in milliseconds) of the TCP user.
per_timer	Value of the persist timer (in milliseconds) of the TCP user.
rt_timer	Value of the retransmit timer (in milliseconds) of the TCP user.
tries	Retransmit count of the TCP user.

Examples

This example shows how to display the status of the TCP stack on the ASA:

```
ciscoasa# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160
tcp_xmt pkts = 540591
```

```
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0
lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

Related Commands

Command	Description
show conn	Displays the connections used and those that are available.

show tech-support

To display the information that is used for diagnosis by technical support analysts, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**detail** [**vsn**] | **file** | **no-config** | **no-config** | **performance**]

Syntax Description

detail	(Optional) Lists detailed information.
file	(Optional) Writes the output of the command to a file. File system types include the following: disk0:, disk1:, ftp:, scp:, smb:, and tftp:.
no-config	(Optional) Excludes the output of the running configuration.
performance	(Optional) Displays performance information.
vsn	(Optional) Includes additional ASA1000V Policy Agent technical support information, which is redirected to a file.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	The **detail** and **file** keywords were added.
7.2(1)	The output was enhanced to display more detailed information about processes that hog the CPU.
9.1(2)	The output was enhanced to include information from the **show environment** command.
9.1(3)	The output was enhanced to include information from the **show memory detail, show memory top-usage,** and **show vlan** commands.
9.2(1)	The output was enhanced to include information from the **show memory detail** , **show cpu detail** , **show blocks queue history core-local** , **show asp drop** , and **show asp event dp-cp** , **show cpu usage history** , and **show traffic summary** commands. The output from the **show kernel cgroup-controller detail** command was removed.The **performance** and **vsn** keywords were added.
9.2(1)	The output was enhanced to include information from the **show vlan** command.

Release	Modification
9.1(7)/9.3(1)	The **show tech-support** command now includes **show resource usage count all 1** output, including information about xlates, conns, inspects, syslogs, and so on. This information is helpful for diagnosing performance issues.
9.3(2)	The **show route-summary** command output was added to the **show tech-support detail** command.
9.4(1)	The **show tech-support** command output includes the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.
9.1(7)/9.4(3)/9.5(2)	The **show tech-support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the following cases: • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail** .
9.7.(1)	The **show tech-support** command was updated for the following changes: • The output was enhanced to include crashinfo statistics like **thread name** , **registry content** , **timestamp** , and **traceback** from the crashed thread. The output from **Saved crash** timestamp was removed. • The output was enhanced to include **show ipsec stats** , **show crypto ikev1 stats** , and **show crypto ikev2 stats** commands. These commands are used to gather VPN statistics for troubleshooting purposes. • The **show tech-support** command now includes **show vm** output. It determines the hypervisor on which the ASA virtual is currently running. This information is helpful for performing multiple automated checks on virtual platforms. • The **show tech-support** command now includes **show module detail** command. This command provides information about multiple modules, which is helpful for troubleshooting various connectivity and status issues.
9.12(1)	The output of **show ipv6 interface, show aaa-server, and show fragment** was added to the output of **show tech-support** .
9.13(1)	The **show flow-offload info detail, show flow-offload statistics** , and **show asp table socket** commands were added.
9.14(1)	The **show ssl objects and show ssl errors was added to the output of show tech-support.** Also in 9.12(4)

Release	Modification
9.16(1)	The **show tech-support** command is enhanced for the following changes: • **showcontroller** command output that includes DPDK log messages from the last boot. • **meminfo** statistics about the virtual machine's (VM) free and used memory, shared memory, and buffers. • **cmdline** statistics about the options and arguments passed during boot.
9.17(1)	The output from **show access-list element-count** and **show asp rule-engine** were added. The output of the **show tech-support** command now includes the current DPDK memory pool statistics.
9.20(2)	The output of this command includes the output for **statistics all**,**statistics events**,**statistics np-clients**,**statistics cp-clients**, and **statistics bulk-sync** statistics.

Usage Guidelines

The show tech-support command lets you list information that technical support analysts need to help you diagnose problems. This command combines the output from the show commands that provide the most information to a technical support analyst.

Examples

The following example shows how to save the **show tech-support** output to a file on disk0. The output is extremely long, so if you send the results to your screen, it will take a long time to page through the results.

```
ciscoasa# show tech-support file disk0:tech-support-output.txt

ciscocasa#
```

Note Do not use the **terminal pager 0** command while running any show commands, as it can lead to a huge CPU load. The CPU overload can result in ASA communication failure. Hence, use the default config terminal pager settings (25 lines).

Related Commands

Command	Description
show clock	Displays the clock for use with the Syslog Server (PFSS) and the Public Key Infrastructure (PKI) protocol.
show conn count	Displays the connections used and available.
show cpu	Display the CPU utilization information.
show failover	Displays the status of a connection and which ASA is active
show memory	Displays a summary of the maximum physical memory and current free memory that is available to the operating system.

Command	Description
show perfmon	Displays information about the performance of the ASA
show processes	Displays a list of the processes that are running.
show running-config	Displays the configuration that is currently running on the ASA.
show xlate	Displays information about the translation slot.

show telemetry

To view the telemetry data, use the **show telemetry** command in privileged EXEC mode with one of the keywords. It displays the data in JSON format.

show telemetry [**history** | **last-report** | **sample**]

Syntax Description

history	(Optional) Shows the past 100 events related to telemetry configuration and activities.
last-report	(Optional) Shows the latest telemetry data sent to FXOS in JSON format.
sample	(Optional) Shows the instantly generated telemetry data in JSON format.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.13(1)	Command was introduced.

Usage Guidelines

The service telemetry command is enabled by default. You can choose to view the last sent telemetry data or the last 100 events related to telemetry configuration and activities.

Examples

The following is sample output from the **show telemetry history** command:

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 1. Telemetry support on the chassis: disabled
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
```

Related Commands

Command	Description
no service telemetry	Disables the telemetry service.
show running-config	Displays only the non-default telemetry settings that is configured.

Command	Description
show running-config all	Displays the configured telemetry settings.

show terminal

To show the terminal settings for the current CLI session, use the **show terminal** command in privileged EXEC mode.

show terminal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	Command added.

Usage Guidelines

Set the terminal properties with the following commands:

- **terminal interactive**—Enables help in the current CLI session when you enter **?** at the CLI.
- **terminal monitor**—Allows syslog messages to show in the current CLI session.
- **terminal width**—Sets the width for displaying information during console sessions.

The **show terminal** command does not show the **terminal pager** setting.

Examples

The following is sample output from the **show terminal** command:

```
ciscoasa# show terminal
Width = 80, no monitor
terminal interactive
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the "---more---" prompt. This command is saved to the configuration.

Command	Description
show running-config terminal	Displays the current terminal settings.
terminal interactive	Enables help in the current CLI session when you enter **?** at the CLI.
terminal monitor	Allows syslog messages to show in the current CLI session.
terminal pager	Sets the number of lines to display in a Telnet session before the "---more---" prompt. This command is not saved to the configuration.
terminal width	Sets the width for displaying information during console sessions.

show threat-detection memory

To show the memory used by advanced threat detection statistics, which are enabled by the **threat-detection statistics** command, use the **show threat-detection memory** command in privileged EXEC mode.

show threat-detection memory

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

Some statistics can use a lot of memory and can affect ASA performance. This command lets you monitor memory usage so you can adjust your configuration if necessary.

Examples

The following is sample output from the **show threat-detection memory** command:

```
ciscoasa# show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
=============================
Subtotal TD Chunks              70265072
Regular memory                BYTES USED
TD Port                            33824
TD Control block                  162064
=============================
Subtotal Regular Memory           195888
Total TD memory:                70460960
```

Related Commands

Command	Description
show threat-detection statistics host	Shows the host statistics.

Command	Description
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection statistics	Enables advanced threat-detection statistics.

show threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can view statistics using the **show threat-detection rate** command in privileged EXEC mode.

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack**]

Syntax Description

acl-drop	(Optional) Shows the rate for dropped packets caused by denial by access lists.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
bad-packet-drop	(Optional) Shows the rate for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
conn-limit-drop	(Optional) Shows the rate for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	(Optional) Shows the rate for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	(Optional) Shows the rate for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as **interface-drop**, **inspect-drop**, and **scanning-threat**.
icmp-drop	(Optional) Shows the rate for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	(Optional) Shows the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	(Optional) Shows the rate limit for dropped packets caused by an interface overload.
scanning-threat	(Optional) Shows the rate for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	(Optional) Shows the rate for dropped packets caused by an incomplete session, such as TCP SYN attack or UDP session with no return data attack.

Command Default

If you do not specify an event type, all events are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 10 minutes, then the burst interval is 10 seconds. If the last burst interval was from 3:00:00 to 3:00:10, and you use the **show** command at 3:00:15, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection rate** command:

```
ciscoasa# show threat-detection rate
                          Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                  0               0       0                   16
  1-hour ACL  drop:                  0               0       0                  112
  1-hour SYN attck:                  5               0       2                21438
  10-min  Scanning:                  0               0      29                  193
  1-hour  Scanning:                106               0      10               384776
  1-hour Bad  pkts:                 76               0       2               274690
  10-min  Firewall:                  0               0       3                   22
  1-hour  Firewall:                 76               0       2               274844
  10-min DoS attck:                  0               0       0                    6
  1-hour DoS attck:                  0               0       0                   42
  10-min Interface:                0              0       0                 204
  1-hour Interface:               88              0       0              318225
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection scanning-threat

If you enable scanning threat detection with the **threat-detection scanning-threat** command, then view the hosts that are categorized as attackers and targets using the **show threat-detection scanning-threat** command in privileged EXEC mode.

show threat-detection scanning-threat [**attacker | target**]

Syntax Description

attacker	(Optional) Shows attacking host IP addresses.
target	(Optional) Shows targeted host IP addresses.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	The display was modified to include "& Subnet List" in the heading text.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.
9.0	Interface information was added to the output.

Examples

The following is sample output from the **show threat-detection scanning-threat** command:

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
```

```
192.168.10.8 (outside)
192.168.10.9 (outside)
```

Related Commands

Command	Description
clear threat-detection shun	Releases hosts from being shunned.
show threat-detection shun	Shows the currently shunned hosts.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection shun

If you enable scanning threat detection with the **threat-detection scanning-threat** command, and you automatically shun attacking hosts, then view the currently shunned hosts using the **show threat-detection shun** command in privileged EXEC mode.

show threat-detection shun

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.
9.0	Interface information was added to the output.

Usage Guidelines

To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

The following is sample output from the **show threat-detection shun** command:

```
ciscoasa# show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

Related Commands

Command	Description
clear threat-detection shun	Releases hosts from being shunned.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection statistics host

After you enable threat statistics with the **threat-detection statistics host** command, view host statistics using the **show threat-detection statistics host** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

Syntax Description

ip_address	(Optional) Shows statistics for a particular host.
mask	(Optional) Sets the subnet mask for the host IP address.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics host** command:

```
ciscoasa# show threat-detection statistics host
                          Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

Table 13-2 shows each field description.

Table 87: show threat-detection statistics host Fields

Field	Description
Host	Shows the host IP address.
tot-ses	Shows the total number of sessions for this host since it was added to the database.
act-ses	Shows the total number of active sessions that the host is currently involved in.

Field	Description
fw-drop	Shows the number of firewall drops. Firewall drops is a combined rate that includes all firewall-related packet drops tracked in basic threat detection, including access list denials, bad packets, exceeded connection limits, DoS attack packets, suspicious ICMP packets, TCP SYN attack packets, and UDP session with no return data attack packets. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.
insp-drop	Shows the number of packets dropped because they failed application inspection.
null-ses	Shows the number of null sessions, which are TCP SYN sessions that did not complete within the 30-second timeout, and UDP sessions that did not have any data sent by its server 3 seconds after the session starts.
bad-acc	Shows the number of bad access attempts to host ports that are in a closed state. When a port is determined to be in a null session (see above), the port state of the host is set to HOST_PORT_CLOSE. Any client accessing the port of the host is immediately classified as a bad access without the need to wait for a timeout.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Field	Description
20-min, 1-hour, 8-hour, and 24-hour	By default, there are three rate intervals shown. You can reduce the number of rate intervals using the **threat-detection statistics host number-of-rate** command. Because host statistics use a lot of memory, reducing the number of rate intervals from the default of 3 reduces the memory usage. If you set this keyword to 1, then only the shortest rate interval statistics are maintained. If you set the value to 2, then the two shortest intervals are maintained.
Sent byte	Shows the number of successful bytes sent from the host.
Sent pkts	Shows the number of successful packets sent from the host.
Sent drop	Shows the number of packets sent from the host that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the host.
Recv pkts	Shows the number of successful packets received by the host.
Recv drop	Shows the number of packets received by the host that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics port

After you enable threat statistics with the **threat-detection statistics port** command, view TCP and UDP port statistics using the **show threat-detection statistics port** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min-display-rate*] **port** [*start_port* [*-end_port*]]

Syntax Description

start_port [*-end_port*]	(Optional) Shows statistics for a particular port or range of ports, between 0 and 65535.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics port** command:

```
ciscoasa# show threat-detection statistics port
                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939               0       0             10580922
  8-hour Sent byte:                367           22043       0             10580922
 24-hour Sent byte:                122            7347       0             10580922
  1-hour Sent pkts:                 28               0       0               104049
  8-hour Sent pkts:                  3             216       0               104049
 24-hour Sent pkts:                  1              72       0               104049
  20-min Sent drop:                  9               0       2                10855
  1-hour Sent drop:                  3               0       2                10855
  1-hour Recv byte:               2698               0       0              9713376
  8-hour Recv byte:                337           20236       0              9713376
 24-hour Recv byte:                112            6745       0              9713376
  1-hour Recv pkts:                 29               0       0               104853
  8-hour Recv pkts:                  3             218       0               104853
 24-hour Recv pkts:                  1              72       0               104853
  20-min Recv drop:                 24               0       2                29134
  1-hour Recv drop:                  8               0       2                29134
```

Table 13-2 shows each field description.

Table 88: show threat-detection statistics port Fields

Field	Description
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00

Field	Description
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
port_number /port_name	Shows the port number and name where the packet or byte was sent, received, or dropped.
tot-ses	Shows the total number of sessions for this port.
act-ses	Shows the total number of active sessions that the port is currently involved in.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the port.
Sent pkts	Shows the number of successful packets sent from the port.
Sent drop	Shows the number of packets sent from the port that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the port.
Recv pkts	Shows the number of successful packets received by the port.
Recv drop	Shows the number of packets received by the port that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics protocol

After you enable threat statistics with the **threat-detection statistics protocol** command, view IP protocol statistics using the **show threat-detection statistics protocol** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

Syntax Description

protocol_number	(Optional) Shows statistics for a specific protocol number, between 0 and 255.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
protocol_name	(Optional) Shows statistics for a specific protocol name: • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics protocol** command:

```
ciscoasa# show threat-detection statistics protocol
                          Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                  0               0       0                 1000
  8-hour Sent byte:                  0               2       0                 1000
 24-hour Sent byte:                  0               0       0                 1000
  1-hour Sent pkts:                  0               0       0                   10
  8-hour Sent pkts:                  0               0       0                   10
 24-hour Sent pkts:                  0               0       0                   10
```

Table 13-2 shows each field description.

Table 89: show threat-detection statistics protocol Fields

Field	Description
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
protocol_number /*protocol_name*	Shows the protocol number and name where the packet or byte was sent, received, or dropped.
tot-ses	Not currently used.
act-ses	Not currently used.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the protocol.
Sent pkts	Shows the number of successful packets sent from the protocol.
Sent drop	Shows the number of packets sent from the protocol that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the protocol.

Field	Description
Recv pkts	Shows the number of successful packets received by the protocol.
Recv drop	Shows the number of packets received by the protocol that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics host	Shows the host statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics top

After you enable threat statistics with the **threat-detection statistics** command, view the top 10 statistics using the **show threat-detection statistics top** command in privileged EXEC mode. If you did not enable the threat detection statistics for a particular type, then you cannot view those statistics with this command. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list | host | port-protocol**] [**rate-1 | rate-2 | rate-3**] **| tcp-intercept** [**all**] [**detail**] [**long**]]

Syntax Description

access-list	(Optional) Shows the top 10 ACEs that that match packets, including both permit and deny ACEs. Permitted and denied traffic are not differentiated in this display. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command.
all	(Optional) For TCP Intercept, shows the history data of all the traced servers.
detail	(Optional) For TCP Intercept, shows history sampling data.
host	(Optional) Shows the top 10 host statistics for each fixed time period. **Note** Due to the threat detection algorithm, an interface used for a failover link or state link could appear as one of the top 10 hosts. This occurrence is more likely when you use one interface for both the failover and state link. This is expected behavior, and you can ignore this IP address in the display.
long	(Optional) Shows the statistical history in a long format, with the real IP address and the untranslated IP address of the server.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
port-protocol	(Optional) Shows the top 10 combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols; TCP and UDP ports are, however, included in the display for ports. If you only enable statistics for one of these types, port or protocol, then you will only view the enabled statistics.
rate-1	(Optional) Shows the statistics for the smallest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-1** keyword, the ASA shows only the 1 hour time interval.
rate-2	(Optional) Shows the statistics for the middle fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-2** keyword, the ASA shows only the 8 hour time interval.

rate-3	(Optional) Shows the statistics for the largest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-3** keyword, the ASA shows only the 24 hour time interval.
tcp-intercept	Shows TCP Intercept statistics. The display includes the top 10 protected servers under attack.

Command Default

If you do not specify an event type, all events are shown.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	The **tcp-intercept** keyword was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	The **long** keyword was added for **tcp-intercept** . For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

The following is sample output from the **show threat-detection statistics top access-list** command:

```
ciscoasa# show threat-detection statistics top access-list
                   Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]            173               0       0               623488
              200/2[1]             43               0       0               156786
              100/1[2]             43               0       0               156786
  8-hour ACL hits:
              100/3[0]             21            1298       0               623488
              200/2[1]              5             326       0               156786
              100/1[2]              5             326       0               156786
```

Table 13-2 shows each field description.

Table 90: show threat-detection statistics top access-list Fields

Field	Description
Top	Shows the ranking of the ACE within the time period, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 ACEs might be listed.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00.
Trigger	This column is always 0, because there are no rate limits triggered by access list traffic; denied and permitted traffic are not differentiated in this display. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Field	Description
1-hour, 8-hour	Shows statistics for these fixed rate intervals.
acl_name /line_number	Shows the access list name and line number of the ACE that caused the denies.

The following is sample output from the **show threat-detection statistics top access-list rate-1** command:

```
ciscoasa# show threat-detection statistics top access-list rate-1
                   Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
             100/3[0]             173                0       0               623488
             200/2[1]              43                0       0               156786
             100/1[2]              43                0       0               156786
```

The following is sample output from the **show threat-detection statistics top port-protocol** command:

```
ciscoasa# show threat-detection statistics top port-protocol
Top          Name    Id     Average(eps)     Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher    70              71                0       0           32345678
 2  btp-clnt/dhcp    68              68                0       0           27345678
 3         gopher    69              65                0       0           24345678
 4    Protocol-96 * 96              63                0       0           22345678
 5      Port-7314 7314              62                0       0           12845678
 6 BitTorrent/trc  6969              61                0       0           12645678
 7     Port-8191-65535              55                0       0           12345678
 8           SMTP   366              34                0       0            3345678
 9         IPinIP *   4              30                0       0            2345678
10          EIGRP * 88              23                0       0            1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...
Note: Id preceded by * denotes the Id is an IP protocol type
```

Table 13-6 shows each field description.

Table 91: show threat-detection statistics top port-protocol Fields

Field	Description
Top	Shows the ranking of the port or protocol within the time period/type of statistic, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 ports/protocols might be listed.
Name	Shows the port/protocol name.
Id	Shows the port/protocol ID number. The asterisk (*) means the ID is an IP protocol number.
Average(eps)	See the description in Table 13-2.
Current(eps)	See the description in Table 13-2.
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	See the description in Table 13-2.
Time_interval Sent byte	Shows the number of successful bytes sent from the listed ports and protocols for each time period.
Time_interval Sent packet	Shows the number of successful packets sent from the listed ports and protocols for each time period.
Time_interval Sent drop	Shows the number of packets sent for each time period from the listed ports and protocols that were dropped because they were part of a scanning attack.
Time_interval Recv byte	Shows the number of successful bytes received by the listed ports and protocols for each time period.
Time_interval Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
Time_interval Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
port_number /port_name	Shows the port number and name where the packet or byte was sent, received, or dropped.
protocol_number /protocol_name	Shows the protocol number and name where the packet or byte was sent, received, or dropped.

Examples

The following is sample output from the **show threat-detection statistics top host** command:

```
ciscoasa# show threat-detection statistics top host
                   Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]          2938              0        0           10580308
  1-hour Sent pkts:
          10.0.0.1[0]            28              0        0             104043
  20-min Sent drop:
          10.0.0.1[0]             9              0        1              10851
  1-hour Recv byte:
          10.0.0.1[0]          2697              0        0            9712670
  1-hour Recv pkts:
          10.0.0.1[0]            29              0        0             104846
  20-min Recv drop:
          10.0.0.1[0]            42              0        3              50567
  8-hour Sent byte:
          10.0.0.1[0]           367              0        0           10580308
  8-hour Sent pkts:
          10.0.0.1[0]             3              0        0             104043
  1-hour Sent drop:
          10.0.0.1[0]             3              0        1              10851
  8-hour Recv byte:
          10.0.0.1[0]           337              0        0            9712670
  8-hour Recv pkts:
          10.0.0.1[0]             3              0        0             104846
  1-hour Recv drop:
          10.0.0.1[0]            14              0        1              50567
 24-hour Sent byte:
          10.0.0.1[0]           122              0        0           10580308
 24-hour Sent pkts:
          10.0.0.1[0]             1              0        0             104043
 24-hour Recv byte:
          10.0.0.1[0]           112              0        0            9712670
 24-hour Recv pkts:
          10.0.0.1[0]             1              0        0             104846
```

Table 13-7 shows each field description.

Table 92: show threat-detection statistics top host Fields

Field	**Description**
Top	Shows the ranking of the host within the time period/type of statistic, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 hosts might be listed.
Average(eps)	See the description in Table 13-2.
Current(eps)	See the description in Table 13-2.
Trigger	See the description in Table 13-2.
Total events	See the description in Table 13-2.
Time_interval Sent byte	Shows the number of successful bytes sent to the listed hosts for each time period.
Time_interval Sent packet	Shows the number of successful packets sent to the listed hosts for each time period.

Field	Description
Time_interval Sent drop	Shows the number of packets sent for each time period to the listed hosts that were dropped because they were part of a scanning attack.
Time_interval Recv byte	Shows the number of successful bytes received by the listed hosts for each time period.
Time_interval Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
Time_interval Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
host_ip_address	Shows the host IP address where the packet or byte was sent, received, or dropped.

Examples

The following is sample output from the **show threat-detection statistics top tcp-intercept** command:

```
ciscoasa# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
----------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

shows each field description.

Table 93: show threat-detection statistics top tcp-intercept Fields

Field	Description
Monitoring window size:	Shows the period of time over which the ASA samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command. The ASA samples data 30 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 30.
rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.

Field	Description
server_ip:port	Shows the server IP address and the port on which it is being attacked.
interface	Shows the interface through which the server is being attacked.
avg_rate	Shows the average rate of attack, in attacks per second over the sampling period
current_rate	Shows the current attack rate, in attacks per second.
total	Shows the total number of attacks.
attacker_ip	Shows the attacker IP address.
(*last_attack_time* ago)	Shows when the last attack occurred.

Examples

The following is sample output from the **show threat-detection statistics top tcp-intercept long** command with the real source IP address in parentheses:

```
ciscoasa# show threat-detection statistics top tcp-intercept long
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total> <Source
 IP (Last Attack Time)>
--------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

The following is sample output from the **show threat-detection statistics top tcp-intercept detail** command:

```
ciscoasa# show threat-detection statistics top tcp-intercept detail
Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
----------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
     Sampling History (30 Samplings):
             95348      95337      95341      95339      95338      95342
             95337      95348      95342      95338      95339      95340
             95339      95337      95342      95348      95338      95342
             95337      95339      95340      95339      95347      95343
             95337      95338      95342      95338      95337      95342
             95348      95338      95342      95338      95337      95343
             95337      95349      95341      95338      95337      95342
             95338      95339      95338      95350      95339      95570
             96351      96351      96119      95337      95349      95341
             95338      95337      95342      95338      95338      95342
......
```

Table 13-9 shows each field description.

Table 94: show threat-detection statistics top tcp-intercept detail Fields

Field	Description
Monitoring window size:	Shows the period of time over which the ASA samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command. The ASA samples data 30 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 30.
rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
server_ip:port	Shows the server IP address and the port on which it is being attacked.
interface	Shows the interface through which the server is being attacked.
avg_rate	Shows the average rate of attack, in attacks per second over the rate interval set by the **threat-detection statistics tcp-intercept rate-interval** command (by default, the rate interval is 30 minutes). The ASA samples the data every 30 seconds over the rate interval.
current_rate	Shows the current attack rate, in attacks per second.
total	Shows the total number of attacks.
attacker_ip or <various> Last: *attacker_ip*	Shows the attacker IP address. If there is more than one attacker, then “<various>” displays followed by the last attacker IP address.
(*last_attack_time* ago)	Shows when the last attack occurred.
sampling data	Shows all 30 sampling data values, which show the number of attacks at each inerval.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show time-range

To display the configuration of all time range objects, use the **show time-range** command in privileged EXEC mode.

show time-range [[*name*]]

Syntax Description

name	(Optional) Shows information for this time range object only.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

This example shows how to display the configuration of the time range objects. In this example, there is one object, which is named work-hours. Inactive means that the object is not being used.

```
ciscoasa# show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

Related Commands

Command	Description
time-range	Configures time range objects.

show tls-proxy

To display TLS proxy and session information, use the **show tls-proxy** command in global configuration mode.

show tls-proxy [*tls_name* | [**session** [**host** *host_addr* | **detail** [**cert-dump**] | **count** | **statistics**]]]

Syntax Description

cert-dump	Dumps the local dynamic certificate. Output is a hex dump of the LDC.
count	Shows only the session counters.
detail [**cert-dump**]	Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC. Add the **cert-dump** keyword to get a hexadecimal dump of the local dynamic certificate (LDC). You can also use these keywords with the **host** option.
host *host_addr*	Specifies the IPv4 or IPv6 address of a particular host to show the associated sessions associated.
session	Shows active TLS proxy sessions.
statistics	Shows statistics for monitoring and managing TLS sessions.
tls_name	Name of the TLS proxy to show.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(2)	This command was added.
8.3(1)	The **statistics** keyword was added.

Examples

The following is sample output from the **show tls-proxy** command:

```
ciscoasa# show tls-proxy
TLS-Proxy ‘proxy’: ref_cnt 1, seq#1
 Server proxy:
  Trust-point: local_ccm
 Client proxy:
  Local dynamic certificate issuer: ldc_signer
  Local dynamic certificate key-pair: phone_common
  Cipher-suite <unconfigured>
 Run-time proxies:
  Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
   Active sess 1, most sess 4, byte 3244
```

The following is sample output from the **show tls-proxy session** command:

```
ciscoasa# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

The following is sample output from the **show tls-proxy session detail** command:

```
ciscoasa# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
 Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
 Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
 Status: Available
 Certificate Serial Number: 29
 Certificate Usage: General Purpose
 Public Key Type: RSA (1024 bits)
 Issuer Name:
  cn=TLS-Proxy-Signer
 Subject Name:
  cn=SEP0002B9EB0AAD
  o=Cisco Systems Inc
  c=US
 Validity Date:
  start date: 00:47:12 PDT Feb 27 2007
  end   date: 00:47:12 PDT Feb 27 2008
 Associated Trustpoints:
```

The following is sample output from the **show tls-proxy session statistics** command:

```
ciscoasa# show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                         0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                              2
    SCCP:                                            20
    DIAMETER:                                       200
Total TLS Proxy Sessions
    Established:                                    822
    Platform Limit:                                1000
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show running-config tls-proxy	Shows running configuration of all or specified TLS proxies.

Command	Description
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show track

To display information about object tracked by the security-level agreement (SLA) tracking process, use the **show track** command in user EXEC mode.

show track [*track-id*]

Syntax Description

track-id	A tracking entry object ID number, from 1 to 500.

Command Default

If the *track-id* is not provided, then information about all tracking objects is displayed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following is sample output from the **show track** command:

```
ciscoasa(config)# show track
Track 5
 Response Time Reporter 124 reachability
 Reachability is UP
 2 changes, last change 03:41:16
 Latest operation return code: OK
 Tracked by:
  STATIC-IP-ROUTING 0
```

Related Commands

Command	Description
show running-config track	Displays the **track rtr** commands in the running configuration.
track rtr	Creates a tracking entry to poll the SLA.

show traffic

To display interface transmit and receive activity, use the **show traffic** command in privileged EXEC mode.

show traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	Output for the ASA 5550 was added.
9.3(1)	Output for aggregated traffic on physical interfaces was added.
9.5(2)	SCTP and SCTP inspection were added to the detailed output.

Usage Guidelines

The **show traffic** command lists the number of packets and bytes moving through each interface since the last **show traffic** command was entered or since the ASA came online. The number of seconds is the duration the ASA has been online since the last reboot, unless the **clear traffic** command was entered since the last reboot. If this is the case, then the number of seconds is the duration since that command was entered.

For the ASA 5550, the **show traffic** command also shows the aggregated throughput per slot. Because the ASA 5550 requires traffic to be evenly distributed across slots for maximum throughput, this output helps you determine if the traffic is distributed evenly.

To show aggregated traffic on physical interfaces, you must first enter the **sysopt traffic detailed-statistics** command to turn on this feature.

Examples

The following is sample output from the **show traffic** command:

```
ciscoasa# show traffic
outside:        received (in 102.080 secs):                2048 packets 204295 bytes
          20 pkts/sec 2001 bytes/sec        transmitted (in 102.080 secs):
2048 packets 204056 bytes              20 pkts/sec 1998 bytes/secEthernet0:       received
 (in 102.080 secs):                2049 packets 233027 bytes                20 pkts/sec
2282 bytes/sec        transmitted (in 102.080 secs):                2048 packets 232750
bytes                20 pkts/sec 2280 bytes/sec
```

For the ASA 5550, the following text is displayed at the end:

```
----------------------------------------
        Per Slot Throughput Profile
----------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************
  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

The following example shows the added output for aggregated traffic on physical interfaces:

```
IP packet size distribution (values listed in percentages)
Total Packets = 1278:
      32    64    96   128   192   256   512
    00.0  43.5  10.4  10.1  26.1  01.4  03.6

    1024  1536  2048  4096  8192  9216
    03.6  06.6  00.0  00.0  00.0  00.0

Protocol         Total    Conns   Packets   Bytes  Packets    Total
--------         Conns     /Sec     /Conn    /Pkt     /Sec  Packets
```

SCTP 0 0.0 0 0 0 0.0 0

```
SCTP-inspected        0      0.0       N/A     N/A      0.0        0
TCP                  8      0.2        98     215     26.8     1279
TCP-inspected        0      0.0       N/A     N/A      0.0        0
UDP                  3      0.0         0      90      0.0        2
UDP-inspected        5      0.0         1     189      0.0       56
ICMP                 0      0.0         1      98      0.0        2
ESP                   0      0.0       N/A     N/A      0.0        0
IP                   0      0.0       N/A     N/A      0.0        0
Total:              16      0.2        22     207     26.8     1433

Last clearing of statistics: Never
```

Related Commands

Command	Description
clear traffic	Resets the counters for transmit and receive activity.

show u – show z

show uauth

To display one or all currently authenticated users, the host IP to which they are bound, and any cached IP and port authorization information, use the **show uauth** command in privileged EXEC mode.

show uauth [*username*]

Syntax Description

username	(Optional) Specifies, by username, the user authentication and authorization information to display.

Command Default

Omitting username displays the authorization information for all users.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
7.2(1)	The idle time was added to the output.
7.2(2)	The idle time was removed from the output.

Usage Guidelines

The **show uauth** command displays the AAA authorization and authentication caches for one user or for all users.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. The cache allows up to 16 address and service pairs for each user host. If the user attempts to access a service that has been cached from the correct host, the ASA considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, for example, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and if the user is authenticated only or has cached services.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPsec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see to the **aaa** commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows sample output from the **show uauth** command when no users are authenticated and one user authentication is in progress:

```
ciscoasa(config)# show uauth

                        Current    Most Seen
Authenticated Users        1            1
Authen In Progress         0            1
user 'v039294' at 136.131.178.4, authenticated (idle for 0:00:00)
   access-list #ACSACL#-IP-v039294-521b0b8b (*)
   absolute   timeout: 0:00:00
   inactivity timeout: 0:05:00
```

This example shows sample output from the **show uauth** command when three users are authenticated and authorized to use services through the ASA:

```
ciscoasa(config)# show uauth
user ‘pat’ from 209.165.201.2 authenticated
user ‘robin’ from 209.165.201.4 authorized to:
                       port 192.168.67.34/telnet                        192.168.67.11/http
                                    192.168.67.33/tcp/8001
                                                      192.168.67.56/tcp/25
                  192.168.67.42/ftp
user ‘terry’ from 209.165.201.7 authorized to:
                       port 192.168.1.50/http
209.165.201.8/http
```

Related Commands

Command	Description
clear uauth	Removes current user authentication and authorization information.
timeout	Sets the maximum idle time duration.

show url-block

To display the number of packets held in the url-block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission, use the **show url-block** command in privileged EXEC mode.

show url-block [**block statistics**]

Syntax Description

block **statistics**	(Optional) Displays block buffer usage statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show url-block block statistics** command displays the number of packets held in the url block buffer and the number (if any) dropped due to exceeding the buffer limit or retransmission.

Examples

The following is sample output from the **show url-block** command:

```
ciscoasa# show url-block
 | url-block url-mempool 128 | url-block url-size 4 | url-block block 128
```

This shows the configuration of the URL block buffer.

The following is sample output from the **show url-block block statistics** command:

```
ciscoasa# show url-block block statistics
URL Pending Packet Buffer Stats with max block  128 |
Cumulative number of packets held: | 896
Maximum number of packets held (per URL): | 3
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 7546
 | HTTP server retransmission: | 10
Number of packets released back to client: | 0
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show url-cache statistics

To display information about the url-cache, which is used for URL responses received from an N2H2 or Websense filtering server, use the **show url-cache statistics** command in privileged EXEC mode.

show url-cache statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show url-cache statistics** command displays the following entries:

- Size—The size of the cache in kilobytes, set with the **url-cache** *size* option.
- Entries—The maximum number of cache entries based on the cache size.
- In Use—The current number of entries in the cache.
- Lookups—The number of times the ASA has looked for a cache entry.
- Hits—The number of times the ASA has found an entry in the cache.

You can view additional information about N2H2 Sentian or Websense filtering activity with the **show perfmon** command.

Examples

The following is sample output from the show url-cache statistics command:

```
ciscoasa# show url-cache statistics
URL Filter Cache Stats
----------------------
 |
Size :                              1KB
 Entries :                                  36
             In Use :                                  30
 Lookups :                                  300
```

```
  |
Hits :                                    290
```

Related Commands

Commands	Description
clear url-cache statistics	Removes url-cache command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching for responses received from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show url-server

To display information about the URL filtering server, use the **show url-server** command in privileged EXEC mode.

show url-server statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show url-server statistics** command displays the URL server vendor; number of URLs total, allowed, and denied; number of HTTPS connections total, allowed, and denied; number of TCP connections total, allowed, and denied; and the URL server status.

The show url-server command displays the following information:

- For N2H2, **url-server (***if_name***)vendor n2h2host** *local_ip* **port** *number* **timeout** *seconds* **protocol** [{**TCP** | **UDP**}{**version 1** | **4**}]
- For Websense, **url-server (***if_name***)vendor websense host** *local_ip* **timeout** *seconds* **protocol** [{**TCP** | **UDP**}]

Examples

The following is sample output from the **show url-server statistics** command:

```
ciscoasa## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second
URL Server Statistics:
----------------------
192.168.0.1                         UP
Vendor                          websense
Port                            17035
Requests total/allowed/denied   366519/255495/110457
Server timeouts/retries         567/1350
Responses received              365952
Response time average 60s/300s  2/1 seconds/request
192.168.0.2                         DOWN
Vendor                          websense
Port                            17035
Requests total/allowed/denied   0/0/0
Server timeouts/retries         0/0
Responses received              0
Response time average 60s/300s  0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          411     0
LOOKUP_REQUEST          366519  365952
LOG_REQUEST             0       NA
Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0
Semantics:
This command allows the operator to display url-server statistics organized on a global and
 per-server basis. The output is reformatted to provide: more-detailed information and
per-server organization.
Supported Modes:
privileged
router || transparent
single || multi/context
Privilege:
ATTR_ES_CHECK_CONTEXT
Debug support:
N/A
Migration Strategy (if any):
N/A
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.

Commands	Description
url-server	Identifies an N2H2 or Websense server for use with the filter command.

show user-alert

To show the currently configured user alert that can be displayed to all active clientless WebVPN sessions use the show user-alert command in privileged EXEC mode.

show user-alert

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Related Commands

Command	Description
user-alert	Enables broadcast of an urgent message to all clientless SSL VPN users with a currently active session.

show user-identity ad-agent

To display information about the AD Agent for the Identify Firewall, use the **show user-identity ad-agent** command in privileged EXEC mode.

show user-identity ad-agent [**statistics**]

Syntax Description

statistics	(Optional) Displays statistical information about the AD Agent.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

You can monitor the AD Agent component of the Identity Firewall.

Use the **show user-identity ad-agent** command to obtain troubleshooting information for the AD Agent. This command displays the following information about the primary and secondary AD Agents:

- Status of the AD Agents
- Status of the domains
- Statistics for the AD Agents

Table 95: Description of the Command Output

Type	Values	Description
Mode	Configuration mode	Specifies full download or on-demand download.
AD Agent IP Address	IP address	Displays the active AD Agent IP address.
Backup	IP address	Displays the backup AD Agent IP address.

Type	Values	Description
AD Agent Status	• Disabled • Down • Up (registered) • Probing	• The Identity Firewall is disabled. • The AD Agent is down. • The AD Agent is up and running. • The ASA is registered and the AD Agent is up and running. • The ASA is trying to connect to the AD Agent.
Authentication Port	udp/1645	Displays the AD Agent authentication port.
Accounting Port	udp/1646	Displays the AD Agent accounting port.
ASA Listening Port	udp/3799	Displays the ASA listening port.
Interface	Interface	Displays the interface that the ASA uses to contact the AD Agent.
IP Address	IP address	Displays the IP address that the ASA uses to contact the AD Agent.
Uptime	Time	Displays the AD Agent up time.
Average RTT	Milliseconds	Displays the average round trip time the ASA uses to contact the AD Agent.
Domain	Domain nickname Status: up Status: down	Displays the Microsoft Active Directory domain for the AD Agent.

Examples

This example shows how to display information for the AD Agent for the Identify Firewall:

```
ciscoasa# show user-identity ad-agent
Primary AD Agent:
 Status                     up (registered)
 Mode:                      full-download
 IP address:                172.23.62.125
 Authentication port:       udp/1645
 Accounting port:           udp/1646
 ASA Listening port:        udp/3799
 Interface:                 mgmt
 Up time:                   15 mins 41 secs
 Average RTT:               57 msec
Secondary AD Agent:
 Status                     up
 Mode:                      full-download
 IP address:                172.23.62.136
 Authentication port:       udp/1645
 Accounting port:           udp/1646
 ASA Listening port:        udp/3799
 Interface:                 mgmt
 Up time:                   7 mins 56 secs
 Avg RTT:                   15 msec
```

Related Commands

Command	Description
clear user-identity ad-agent statistics	Clears the statistics data of AD Agents maintained by the ASA for the Identity Firewall.
user-identity enable	Creates the Cisco Identify Firewall instance.
show user-identity ad-group-members	Displays the group members in the domain of the AD Agent for the Identify Firewall.

show user-identity ad-group-members

To display the group members in the domain of the AD Agent for the Identify Firewall, use the **show user-identity ad-group-members** command in privileged EXEC mode.

show user-identity ad-group-members [*domain_nickname* \ ] *user_group_name* [**timeout seconds** *seconds*]

Syntax Description

domain_nickname	(Optional) Specifies the domain name for the Identity Firewall.
timeout seconds seconds	(Optional) Sets a timer for retrieving group member statistics and specifies the length of time for the timer.
user_group_name	(Optional) Specifies the group name from which to retrieve statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

The **show user-identity ad-group-members** command displays the immediate members (the users and groups) of the specified user group.

Note This command does not display information for locally defined groups on the ASA configured with the **object-group user** command.

The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server. Running this command is equivalent to running an LDAP browser command that allows you to check members of a specified user group. ASA issues one level of LDAP query to retrieve the immediate members of the specified group in the distinguishedName format. Running this command does not update the ASA internal cache of imported user groups.

When you do not specify *domain_nickname* , the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

The group name is the AD group's unique sAMAccountName not the CN name. To display information for a specific group sAMAccountName, use the **show user-identity ad-groups filter** *filter_string* command to retrieve group's sAMAccountName.

Examples

This example shows how to display members of the group sample1 for the Identity Firewall:

```
ciscoasa# show user-identity ad-group-member group.sample1
Domain:CSCO        AAA Server Group:  CISCO_AD_SERVER
Group Member List Retrieved Successfully
Number of Members in AD Group group.schiang: 12
dn: CN=user1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
dn: CN=user2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.
show user-identity ad-groups	Displays information about the AD Agent for the Identify Firewall.

show user-identity ad-groups

To display information for a specific group for the Identify Firewall, use the **show user-identity ad-groups** command in privileged EXEC mode.

show user-identity ad-groups *domain_nickname* { **filter** *filter_string* **| import-user-group** [**count**] }

Syntax Description

count	(Optional) Displays the number of activated groups.
domain_nickname	Specifies the domain name for the Identity Firewall.
filter *filter_string*	Specifies to displays groups that contain the specified filter string in the CN attribute of the domain controller of the Microsoft Active Directory.
import-user-group	Displays only the activated groups for the Identity Firewall.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

When you run the **show user-identity ad-groups** command, the ASA sends an LDAP query to the Microsoft Active Directory to retrieve all user groups that are part of the specified domain nickname. The argument *domain_nickname* can be the real domain nickname or LOCAL. The ASA only retrieves groups that have the group objectclass attribute. The ASA displays the retrieved groups in distinguishedName format.

When you specify the **filter** *filter_string* keyword and argument, the ASA displays groups that contain the specified filter string in the CN attribute of the domain controller. Because the **access-list** and **object-group** commands only take sAMAccountName, you can run the **show user-identity ad-users filter** *filter_string* command to retrieve the sAMAccountName for a group. When you do not specify **filter** *filter_string* , the ASA displays all Active Directory groups.

When you specify the **import-user-group count** keywords, the ASA displays all Active Directory groups that are activated (because they are part an access-group, import-user-group, or service-policy configuration) and stored in the local database. The ASA only displays the sAMAccountName for the groups.

Examples

These examples show how to display user groups that are part of the specified domain nickname for the Identity Firewall:

```
ciscoasa# show user-identity ad-groups CSCO filter sampleuser1
Domain: CSCO        AAA Server Group:       CISCO_AD_SERVER
Group list retrieved successfully
Number of Active Directory Groups       6
dn: CN=group.reg.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.reg.sampleuser1
dn: CN=group.temp.sampleuser1,OU=Organizational,OU=Cisco Groups,DC=cisco,DC=com
sAMAccountName: group.temp.sampleuser1
...
ciscoasa# show user-identity ad-groups CSCO import-user-group count
Total AD groups in domain CSCO stored in local: 2
ciscoasa# show user-identity ad-groups CSCO import-user-group

Domain: CSCO
Groups:
        group.SampleGroup1
        group.SampleGroup2
...
```

This example shows how to run the command to apply a filter string to the results from an access-list and object-group command. Running the **show user-identity ad-users CSCO filter SampleGroup1** command obtains the sAMAccountName of specified string:

```
ciscoasa# show user-identity ad-users CSCO filter SampleGroup1

Domain:CSCO    AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
Number of Active Directory Users: 2
dn: CN=SampleUser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: SampleUser2
dn: CN=SAMPLEUSER2-WXP05,OU=Workstations,OU=Cisco Computers,DC=cisco,DC=com
sAMAccountName: SAMPLEUSER2-WXP05$
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity ad-users

To display Microsoft Active Directory users for the Identify Firewall, use the **show user-identity ad-users** command in privileged EXEC mode.

show user-identity ad-users *domain_nickname* [**filter** *filter_string*]

Syntax Description

domain_nickname	Specifies the domain name for the Identity Firewall.
filter *filter_string*	(Optional) Specifies to displays users that contain the specified filter string in the CN attribute of the domain controller of the Microsoft Active Directory.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

When you run the **show user-identity ad-users** command, the ASA sends an LDAP query to the Microsoft Active Directory to retrieve all users that are part of the specified domain nickname. The argument *domain_nickname* can be the real domain nickname or LOCAL.

When you specify the **filter** *filter_string* keyword and argument, the ASA displays users that contain the specified filter string in the CN attribute of the domain controller. The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server.

The ASA only retrieves users that have the user objectclass attribute and the samAccountType attribute 805306368. Other objects, such as machine objects, can be included in the user objectclass; however, the samAccountType 805306368 filters out the non-user objects. When you do not specify a filter string, the ASA displays all Active Directory users.

The ASA displays the retrieved users in distinguishedName format.

Examples

This example shows how to display information about Active Directory users for the Identity Firewall:

```
ciscoasa# show user-identity ad-users CSCO filter user
Domain: CSCO        AAA Server Group:  CISCO_AD_SERVER
User list retrieved successfully
```

```
Number of Active Directory Users: 10
dn: CN=sampleuser1,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser1
dn: CN=sampleuser2,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: sampleuser2
dn: CN=user3,OU=Employees,OU=Cisco Users,DC=cisco,DC=com
sAMAccountName: user3
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity group

To display the user groups configured for the Identify Firewall, use the **show user-identity group** command in privileged EXEC mode.

show user-identity group

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity group** command to obtain troubleshooting information for the user groups configured for the Identity Firewall. The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server. This command displays the list of activated user groups in the following format:

domain \group_name

The ASA only displays top groups that are applied to a security policy. The maximum number of activated top groups is 256. Groups are activated when they are part an access-group, import-user-group, or service-policy configuration.

Examples

This example shows how to display the activated groups for the Identity Firewall:

```
ciscoasa# show user-identity group
Group ID        Activated Group Name (Domain\\Group)
--------        ------------------------------------
       1        LOCAL\\og1
       2        LOCAL\\marketing
       3        CISCO\\group.sampleuser1
       4        IDFW\\grp1
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity ip-of-user

To display the IP address for a specified user for the Identify Firewall, use the **show user-identity ip-of-user** command in privileged EXEC mode.

show user-identity ip-of-user [*domain_nickname* \ ] *user-name* [**detail**]

Syntax Description

detail	(Optional) Displays the detailed output about the user and IP address.
domain_nickname	(Optional) Specifies the domain name for the Identity Firewall.
user-name	Specifies the user for which to obtain an IP address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

This command displays user information and the IP addresses for the specified user. Users can have more than one IP address associated with them.

When you do not specify the *domain_nickname* argument, the ASA displays information for the user with *user_name* in default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

When you specify the **detail** keyword, the ASA displays the total number of active connections, the user-statistics period and the drops, and the input packets and output packets during the period over all IP addresses for the specified user. When you do not specify the **detail** option, the ASA displays only the domain nickname and status of each IP address.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

These examples show how to display IP addresses of specified users for the Identity Firewall:

```
ciscoasa# show user-identity ip-of-user sampleuser1
CSCO\172.1.1.1 (Login)
CSCO\172.100.3.23 (Login)
CSCO\10.23.51.3 (Inactive)
ciscoasa# show user-identity ip-of-user sampleuser1 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 2 active conns
CSCO\172.100.3.23 (Login) Login time: 20 mins;  Idle time: 10 mins; 10 active conns
CSCO\10.23.51.3 (Inactive) Login time: 3000 mins;  Idle time: 2040 mins; 8 active conns
Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
ciscoasa# show user-identity ip-of-user sampleuser2
ERROR: no such user
ciscoasa# show user-identity ip-of-user sampleuser3
ERROR: no IP address, user not login now
```

IPv6 support

```
ciscoasa# show user-identity ip-of-user sampleuser4
CSCO\172.1.1.1 (Login)
CSCO\8080:1:3::56 (Login)
CSCO\8080:2:3::34 (Inactive)
ciscoasa# show user-identity ip-of-user sampleuser4 detail
CSCO\172.1.1.1 (Login) Login time: 1440 mins;  Idle time: 10 mins; 8 active conns
CSCO\8080:1:3::56 (Login) Login time: 20 mins;  Idle time: 10 mins; 12 active conns
CSCO\8080:2:3::34 (Inactive) Total number of active connections: 20
1-hour recv packets: 12560
1-hour sent packets: 32560
20-min drops: 560
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.
show user-identity user-of-ip	Displays the user information associated with the specified IP address

show user-identity memory

To display the memory of various modules of the Identify Firewall, use the **show user-identity memory** command in privileged EXEC mode.

show user-identity memory

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

You can monitor the memory usage that the Identity Firewall consumes on the ASA. Running the s**how user-identity memory** command displays the memory for user records, group records, host records, and their associated hash table. The ASA also displays the memory used by the identity-based tmatch table.

The command displays the memory usage in bytes of various modules in the Identity Firewall:

- Users
- Groups
- User Statistics
- LDAP

The ASA sends an LDAP query for the Active Directory groups configured on the Active Directory server. The Active Directory server authenticates users and generates user logon security logs.

- AD Agent
- Miscellaneous
- Total Memory Usage

How you configure the Identity Firewall to retrieve user information from the AD Agent impacts the amount of memory used by the feature. You specify whether the ASA uses on demand retrieval or full download retrieval. Selecting On Demand has the benefit of using less memory as only users of received packets are queried and stored. See "Configuring Identity Options" in the CLI configuration guide for a description of these options.

Examples

This example shows how to display the memory status of the modules of the Identity Firewall:

```
ciscoasa# show user-identity memory
Users:       22416048 bytes
Groups:           320 bytes
User stats:         0 bytes
LDAP:             300 bytes
AD agent:         500 bytes
Misc:           32428 bytes
Total:       22449596 bytes
Users:       22416048 bytes
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity statistics

To display statistics for a user or user group for the Identify Firewall, use the **show user-identity statistics** command in privileged EXEC mode.

show user-identity statistics [**user** [*domain_nickname* \ ] *user_name* | **user-group** [*domain_nickname* \ ] *user_group_name*]

Syntax Description

domain_nickname	(Optional) Specifies the domain name for the Identity Firewall.
user *user_name*	(Optional) Specifies the user name from which to retrieve statistics.
user-group *domain_nickname\user_group_name*	(Optional) Specifies the group name from which to retrieve statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Run the show **user-identity statistics** command to display the statistics for a user or user group.

When you do not specify the *domain_nickname* argument with the **user** keyword, the ASA displays information for the user with *user_name* in default domain.

When you do not specify *domain_nickname* with the **user-group** keyword, the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

Examples

These examples show how to display statistics about users for the Identity Firewall:

```
ciscoasa# show user-identity statistics user

Current monitored users:11  Total not monitored users:0
                          Average(eps)    Current(eps) Trigger      Total events
User: CSCO\user1 tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
```

```
  20-min Recv attack:               4              10      14             4861
    1-hour Recv pkts:                 1              10        0              4901
User: CSCO\user2 tot-ses:2456 act-ses:607 fw-drop:0 insp-drop:0 null-ses:2431 bad-acc:0
  20-min Sent attack:                4              10        4              4862
  1-hour Sent pkts:                    0               5         0              2451
...
ciscoasa# show user-identity statistics user user1
Current                          Average(eps)    Current(eps) Trigger      Total events
User: -(user1-) tot-ses:4911 act-ses:1213 fw-drop:0 insp-drop:0 null-ses:4861 bad-acc:0
  20-min Recv attack:               4              10       14              4861
  1-hour Recv pkts:                  1              10       0              4901
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity statistics top user

To display statistics for the top 10 users for the Identify Firewall, use the **show user-identity statistics top user** command in privileged EXEC mode.

show user-identity statistics top user

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

The **show user-identity statistics top user** command displays statistics for received EPS packets, sent EPS packets, and sent attacks for the top 10 users. For each user (displayed as *domain* *user_name*), the ASA displays the average EPS packet, the current EPS packet, the trigger, and total events for that user.

Examples

This example shows how to display information about the top 10 users for the Identity Firewall:

```
ciscoasa# show user-identity statistics top user
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv pkts:
01    APAC\sampleuser1
                                    0               0       0              391
  1-hour Sent pkts:
01    APAC\sampleuser2
                                    0               0       0              196
02    CSCO\sampleuser3
                                    0               0       0              195
  10-min Sent attack:
01    CSCO\sampleuser4
                                    0               0       0              352
02    CSCO\sampleuser3
                                    0               0       0              350
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user active

To display the active users for the Identify Firewall, use the **show user-identity user active** command in privileged EXEC mode.

show user-identity user active [**domain** *domain_nickname* **| user-group** [*domain_nickname* \ ] *user_group_name* **| user** [*domain_nickname* \ ] *user_name*] [**list** [**detail**]]

Syntax Description

detail	(Optional) Displays the detailed output of the active user sessions.
domain *domain_nickname*	Displays statistics for the active users in a specified domain.
list	(Optional) Displays a list summarizing the active user statistics.
user *domain_nickname\ user_name*	(Optional) Displays statistic for a specified user.
user-group *domain_nickname\ user_group_name*	(Optional) Displays statistics for a specified user group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

You can display information about all users contained in the IP-user mapping database used by the Identity Firewall.

The **show user-identity user active** command displays the following information for users:

- *domain \user_name*
- Active Connections
- Minutes Idle

The default domain name can be the real domain name, a special reserved word, or LOCAL. The Identity Firewall uses the LOCAL domain name for all locally defined user groups or locally defined users (users who log in and authenticate by using a VPN or web portal). When default domain is not specified, the default domain is LOCAL.

A user's name is appended with the number of minutes idle. The login time and idle time are stored on a per user basis instead of per the IP address of a user.

When the **user-group** keyword is specified, only the activated user-groups are displayed. Groups are activated when they are part an access-group, import-user-group, or service-policy configuration.

When you do not specify *domain_nickname* with the **user-group** keyword, the ASA displays information for the group that has *user_group_name* in the default domain.

Note When the **user-identity action domain-controller-down** is configured with the **disable-user-identity-rule** keyword and the specified domain is down, or when **user-identity action ad-agent-down** command is configured with the **disable-user-identity-rule** keyword and the AD agent is down, all the logged on users are displayed as disabled in the user statistics.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

The following examples show how to display information about active users for the Identity Firewall:

```
ciscoasa# show user-identity user active

Total active users: 30  Total IP addresses: 35
  LOCAL: 0 users, 0 IP addresses
  cisco.com: 0 users, 0 IP addresses
  d1: 0 users, 0 IP addresses
  IDFW: 0 users, 0 IP addresses
  idfw.com: 0 users, 0 IP addresses
  IDFWTEST: 30 users, 35 IP addresses
ciscoasa# show user-identity user active domain CSCO

Total active users: 48020 Total IP addresses:10000
  CSCO: 48020 users, 10000 IP addresses
ciscoasa# show user-identity user active domain CSCO list

Total active users: 48020 Total IP addresses: 10000
  CSCO: 48020 users, 10000 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 5 mins
   CSCO\member-2: 20 active conns; idle 20 mins
   CSCO\member-3: 3 active conns; idle 101 mins
   ...
ciscoasa# show user-identity user active list

Total active users: 48032  Total IP addresses: 10000
   CSCO\sampleuser1: 20 active conns; idle 0 mins
   CSCO\member-1: 20 active conns; idle 6 mins
   APAC\sampleuser2: 20 active conns; idle 0 mins
   CSCO\member-2: 20 active conns; idle 1 mins
   CSCO\member-3: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 22 mins
   CSCO\member-4: 3 active conns; idle 101 mins
   ...
ciscoasa# show user-identity user active list detail

Total active users: 48032 Total IP addresses: 10010
  CSCO: 48020 users, 10000 IP addresses
  APAC: 12 users, 10 IP addresses
   CSCO\sampleuser1: 20 active conns; idle 0 mins
     172.1.1.1: login 360 mins, idle 0 mins, 15 active conns
     172.100.3.23: login 200 min, idle 15 mins , 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
   CSCO\member-1: 4 active connections;  idle 350 mins
   ...
  APAC\sampleuser12: 3 active conns; idle 101 mins
     172.1.1.1: login 360 mins, idle 101 mins, 1 active conns
     172.100.3.23: login 200 min, idle 150 mins, 2 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
ciscoasa# show user-identity user active list detail
Total users: 25  Total IP addresses: 5
   LOCAL\idfw: 0 active conns
    6.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
    20.0.0.3: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser4: 0 active conns; idle 0 mins
    20.0.0.2: login 0 mins, idle 0 mins, 0 active conns (disabled)
  cisco.com\sampleuser5: 0 active conns
  ...
ciscoasa# show user-identity user active user sampleuser1 list detail

CSCO\sampleuser1: 20 active conns; idle 3 mins
     172.1.1.1: login 360 mins, idle 20 mins, 15 active conns
     172.100.3.23: login 200 mins, idle 3 mins, 5 active conns
     10.23.51.3: inactive
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
ciscoasa# show user-identity user active user APAC\sampleuser2

APAC\sampleuser2: 20 active conns; idle 2 mins
ciscoasa# show user-identity user active user-group APAC\\marketing list

   APAC\sampleuser1: 20 active conns; idle 2 mins
   APAC\member-1: 20 active conns; idle 0 mins
   APAC\member-2: 20 active conns; idle 0 mins
   APAC\member-3: 20 active conns; idle 6 mins
...
ciscoasa# show user-identity user active user-group APAC\\inactive list
ERROR: group is not activated
```

Related Commands

Command	Description
clear user-identity active-user-database	Sets the status of a specified user, all users belong to a specified user group, or all users to logged out for the Identity Firewall.

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user all

To display statistics about users for the Identify Firewall, use the **show user-identity user all** command in privileged EXEC mode.

show user-identity user all [**list**] [**detail**]

Syntax Description

detail	(Optional) Displays the detailed output about all users for the Identity Firewall.
list	(Optional) Displays a list summarizing the statistics for all users for the Identity Firewall.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the show user-identity all command to display information for all users contained in the IP-user mapping database used by the Identity Firewall.

When you include the detail keyword with this command and the command output shows an IP address is inactive, the IP address is not associated with the user. Searching for the user associated with that IP address will return an error.

Note When the **user-identity action domain-controller-down** is configured with the **disable-user-identity-rule** keyword and the specified domain is down, or when **user-identity action ad-agent-down** command is configured with the **disable-user-identity-rule** keyword and the AD agent is down, all the logged on users are displayed as disabled in the user statistics.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

The following examples show how to display statistics about all users for the Identity Firewall:

```
ciscoasa# show user-identity user all list
Total inactive users: 1201  Total IP addresses: 100
ciscoasa# show user-identity user all list
Total users: 7
  LOCAL\idfw: 0 active conns
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns
  cisco.com\sampleuser4: 0 active conns; idle 300 mins
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
  cisco.com\sampleuser7: 0 active conns
ciscoasa# show user-identity user all list detail
Total users: 7 Total IP addresses: 3
  LOCAL\idfw: 0 active conns
    10.1.1.1: inactive
  cisco.com\sampleuser1: 0 active conns
  cisco.com\sampleuser2: 0 active conns
  cisco.com\sampleuser3: 0 active conns; idle 300 mins
    171.69.42.8: inactive
    10.0.0.2: login 300 mins, idle 300 mins, 5 active conns
  cisco.com\sampleuser4: 0 active conns
  cisco.com\sampleuser5: 0 active conns
  cisco.com\sampleuser6: 0 active conns
     1-hour recv packets: 12560
     1-hour sent packets: 32560
     20-min drops: 560
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user inactive

To display information about the inactive users for the Identify Firewall, use the **show user-identity user inactive** command in privileged EXEC mode.

show user-identity user inactive [**domain** *domain_nickname* | **user-group** [*domain_nickname* \ ] *user_group_name*]

Syntax Description

domain *domain_nickname*	(Optional) Displays statistics for the inactive users in the specified domain name for the Identity Firewall.
user-group *domain_nickname\user_group_name*	(Optional) Displays statistics for the inactive users in the specified user group.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user inactive** command to display information about users who have no active traffic for longer than the value configured with the **user-identity inactive-user-timer** command.

When the **user-group** keyword is specified, only the activated user-groups are displayed. Groups are activated when they are part an access-group, import-user-group, or service-policy configuration.

When you do not specify *domain_nickname* with the **user-group** keyword, the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

Examples

These examples show how to display the status of inactive users for the Identity Firewall:

```
ciscoasa# show user-identity user inactive
Total inactive users: 1201
   APAC\sampleuser1
   CSCO\sampleuser2
172.1.1.1: inactive     ...
...
```

```
ciscoasa# show user-identity user inactive domain CSCO
Total inactive users: 1101
    CSCO: 1101
   CSCO\sampleuser1
   CSCO\sampleuser2
   CSCO\sampleuser3
...
ciscoasa# show user-identity user inactive user-group CSCO\\marketing
Total inactive users: 21
   CSCO\sampleuser1
   CSCO\sampleuser2
...
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.
user-identity inactive-user-timer	Specifies the amount of time before a user is considered idle for the Cisco Identify Firewall instance.

show user-identity user-not-found

To display the IP addresses of the Active Directory users not found for the Identify Firewall, use the **show user-identity user-not-found** command in privileged EXEC mode.

show user-identity user-not-found

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user-not-found** command to display the IP addresses of the users who are not found in Microsoft Active Directory.

The ASA maintains a local user-not-found database of these IP addresses. The ASA keeps only the last 1024 packets (contiguous packets from the same source IP address are treated as one packet) of the user-not-found list and not the entire list in the database.

Examples

This example shows how to display information about not-found users for the Identity Firewall:

```
ciscoasa# show user-identity user-not-found
172.13.1.2
171.1.45.5
169.1.1.2
172.13.12
...
```

Related Commands

Command	Description
clear user-identity user-not-found	Clears the ASA local user-not-found database for the Identity Firewall.
user-identity enable	Creates the Cisco Identify Firewall instance.
user-identity user-not-found	Enables user-not-found tracking for the Identify Firewall.

show user-identity user-of-group

To display the users of a specified user group for the Identify Firewall, use the **show user-identity user-of-group** command in privileged EXEC mode.

show user-identity user-of-group [*domain_nickname* \ ] *user_group_name*

Syntax Description

domain_nickname	Specifies the domain name for the Identity Firewall.
user_group_name	Specifies the user group for which to display statistics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user-of-group** command to display users whose group ID matches the specified user group. (The ASA scans the IP-user hash list for this information and rather than sending an LDAP query to Active Directory. The AD Agent maintains a cache of user ID and IP address mappings and notifies the ASA of changes.)

The user group name you specify must be activated, meaning the group is an import user group (defined as a user group in an access list or service policy configuration) or a local user group (defined in an object-group user).

The group can have more than one user member. The members of the user group are all immediate members (including users and groups) of the specified group.

When you do not specify *domain_nickname* with the *user_group_name* argument, the ASA displays information for the group that has *user_group_name* in the default domain. The argument *domain_nickname* can be the real domain nickname or LOCAL.

When the command out put indicates a user's status is inactive, the user can be logged out or has never logged in.

Examples

These examples show how to display users of a specified user group for the Identity Firewall:

```
ciscoasa# show user-identity user-of-group group.samplegroup1
Group: CSCO\\group.user1 Total users: 13
CSCO\user2 10.0.0.10(Login) 20.0.0.10(Inactive) ...
CSCO\user3 10.0.0.11(Inactive)
CSCO\user4 10.0.0.12 (Login)
CSCO\user5 10.0.0.13 (Login)
CSCO\user6 10.0.0.14 (Inactive)
....
ciscoasa# show user-identity user-of-group group.local1
Group: LOCAL\\group.local1    Total users: 2
CSCO\user1 10.0.4.12 (Login)
LOCAL\user2 10.0.3.13 (Login)
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show user-identity user-of-ip

To display information about a user with a specific IP address for the Identify Firewall, use the **show user-identity user-of-ip** command in privileged EXEC mode.

show user-identity user-of-ip *ip_address* [**detail**]

Syntax Description

detail	(Optional) Displays the detailed output about user with the specified IP address.
ip_address	Indicates the IP address of the user for which to display information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	The command was added.

Usage Guidelines

Use the **show user-identity user-of-ip** command to display the user information associated with the specified IP address.

When you specify the **detail** keyword, the ASA displays user login time, idle time, the number of active connections, the user-statistics period and the drops, and the input packets and output packets during the period. When you do not specify the **detail** keyword, the ASA only displays the domain nickname, user name, and status.

When user status is inactive, the user can be logged out or has never logged in.

When you include the **detail** keyword with this command and the command output for an IP address displays an error, the IP address is inactive, meaning that the IP address is not associated with a user.

Note The ASA displays detailed user statistics, such as received packets, sent packets and drops in the specified time period, only when you enable user-statistics scanning or accounting for the Identity Firewall. See the CLI configuration guide for information about configuring the Identity Firewall.

Examples

These examples show how to display the status of the active users for the Identity Firewall:

```
ciscoasa# show user-identity user-of-ip 172.1.1.1
CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 172.1.1.1 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 172.1.2.2 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 172.1.7.7
ERROR: no user with this IP address
```

IPv6 Support

```
ciscoasa# show user-identity user-of-ip 8080:1:1::4

CSCO\sampleuser1 (Login)
ciscoasa# show user-identity user-of-ip 8080:1:1::4 detail
CSCO\sampleuser1 (Login) Login time: 240 mins;  Idle time: 10 mins
Number of active connections: 20
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 8080:1:1::6 detail
CSCO\sampleuser2 (Login) Login time: 1440 mins; Idle time: 100 mins
Number of active connections: 0
1-hour sent packets: 3678
1-hour rcvd packets: 1256
20-min sent drops: 60
ciscoasa# show user-identity user-of-ip 8080:1:1::100
ERROR: no user with this IP address
```

Related Commands

Command	Description
user-identity enable	Creates the Cisco Identify Firewall instance.

show version

To display the software version, hardware configuration, license key, and related uptime data, use the **show version** command in user EXEC mode.

show version

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
User EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.2(1)	In stateful failover mode, an additional line showing cluster uptime is displayed.
8.3(1)	The output now includes whether a feature uses the permanent or time-based key, as well as the duration of the time-based key in use.
8.4(1)	Support for No Payload Encryption models (NPE) was added.
9.3(2)	If REST API Agent is enabled, its version number is displayed.
9.17(1)	Information on how long it took to start (boot) up the system was added to the output.

Usage Guidelines

The show version command allows you to display the software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number (BIOS ID), activation key value, license type, and time stamp for when the configuration was last modified.

If the REST API Agent is installed and enabled, its version number is also displayed.

The serial number listed with the show version command is for the flash partition BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the show version command, not the chassis number.

The failover cluster uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value continues to increase as long as the active unit continues to operate. Therefore, it is possible for the failover cluster uptime to be greater than the individual unit uptime. If you temporarily disable failover, and then reenable it, the failover cluster uptime reports the time the unit was up before failover was disabled plus the time the unit was up while failover was disabled.

If you have a No Payload Encryption model, then when you view the license, VPN and Unified Communications licenses will not be listed.

For the Total VPN Peers on the ASA 5505, the total combined number of VPN sessions of all types depends on your licenses. If you enable AnyConnect Essentials, then the total is the model maximum of 25. If you enable AnyConnect Premium, then the total is the AnyConnect Premium value plus the Other VPN value, not to exceed 25 sessions. Unlike other models, where the Other VPN value equals the model limit for all VPN sessions, the ASA 5505 has a lower Other VPN value than the model limit, so the total value can vary depending on the AnyConnect Premium license.

Examples

The following is sample output from the **show version** command, and shows the software version, hardware configuration, license key, and related uptime information. Note that in an environment where stateful failover is configured an additional line showing the failover cluster uptime is displayed. If failover is not configured, the line is not displayed. This display shows a warning message about minimum memory requirements.

```
*************************************************************************
**                                                                     **
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING ***   **
**                                                                     **
**          ----> Minimum Memory Requirements NOT Met! <----           **
**                                                                     **
**  Installed RAM:  512 MB                                             **
**  Required  RAM: 2048 MB                                             **
**  Upgrade part#: ASA5520-MEM-2GB=                                    **
**                                                                     **
**  This ASA does not meet the minimum memory requirements needed to   **
**  run this image. Please install additional memory (part number      **
**  listed above) or downgrade to ASA version 8.2 or earlier.          **
**  Continuing to run without a memory upgrade is unsupported, and     **
**  critical system features will not function properly.               **
**                                                                     **
*************************************************************************
Cisco Adaptive Security Appliance Software Version 8.4(1)
Device Manager Version 6.4(1)
Compiled on Thu 20-Jan-12 04:05 by builders
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/tomm_backup.cfg"

asa3 up 3 days 3 hours
Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 64MB
Slot 1: ATA Compact Flash, 128MB
BIOS Flash AT49LW080 @ 0xfff00000, 1024KB
Encryption hardware device : Cisco ASA-55x0 on-board accelerator (revision 0x0)
                             Boot microcode   : CN1000-MC-BOOT-2.00
                             SSL/IKE microcode: CNLite-MC-SSLm-PLUS-2.03
                             IPsec microcode  : CNlite-MC-IPSECm-MAIN-2.06
 0: Ext: GigabitEthernet0/0  : address is 0013.c480.82ce, irq 9
 1: Ext: GigabitEthernet0/1  : address is 0013.c480.82cf, irq 9
 2: Ext: GigabitEthernet0/2  : address is 0013.c480.82d0, irq 9
 3: Ext: GigabitEthernet0/3  : address is 0013.c480.82d1, irq 9
 4: Ext: Management0/0       : address is 0013.c480.82cd, irq 11
 5: Int: Not used            : irq 11
 6: Int: Not used            : irq 5
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
```

```
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual
This platform has a Base license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
Serial Number: JMX0938K0C0
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Configuration register is 0x1
Configuration last modified by docs at 15:23:22.339 EDT Fri Oct 30 2012
```

The following message appears if you enter the **show version** command after the **eject** command has been executed, but the device has not been physically removed:

```
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
```

Starting with version 9.17(1), you can see how long it took to boot up the system. The information is after status of how long the system has been running.

```
FP2130-2# show version
Cisco Adaptive Security Appliance Software Version 99.17(1)144
SSP Operating System Version 82.11(1.288i)
Device Manager Version 88.31(0)45

Compiled on Tue 06-Apr-21 05:41 GMT by builders
System image file is "disk0:/mnt/boot/installables/switch/fxos-k8-fp2k-npu.82.11.1.288i.SSB"
Config file at boot was "startup-config"

FP2130-2 up 1 day 23 hours
Start-up time 2 mins 40 secs

Hardware:   FPR-2130, 13703 MB RAM, CPU MIPS 1200 MHz, 1 CPU (12 cores)


 1: Int: Internal-Data0/1    : address is 000f.b748.4800, irq 0
 3: Int: Not licensed        : irq 0
 4: Ext: Management1/1       : address is 2cf8.9b36.0759, irq 0
 5: Int: Internal-Data1/1    : address is 0000.0100.0001, irq 0

License mode: Smart Licensing

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited
Maximum VLANs                     : 1024
Inside Hosts                      : Unlimited
Failover                          : Active/Active
```

```
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Disabled
Security Contexts                 : 2
Carrier                           : Disabled
AnyConnect Premium Peers          : 7500
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 7500
Total VPN Peers                   : 7500
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 8000
Cluster                           : Disabled

Serial Number: JAD232913UX
Configuration register is 0x1
Configuration has not been modified since last system restart.
```

Related Commands

Command	Description
eject	Allows shutdown of external compact flash device before physical removal from the ASA.
show hardware	Displays detail hardware information.
show serial	Displays the hardware serial information.
show uptime	Displays how long the ASA has been up.

show vlan

To display all VLANs configured on the ASA, use the show vlan command in privileged EXEC mode.

show vlan [**mapping** [*primary_id*]]

Syntax Description

mapping	(Optional) Shows the secondary VLANs mapped to the primary VLAN.
primary_id	(Optional) Shows secondary VLANs for a specific primary VLAN.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.2(1)	This command was added.
9.5(2)	The **mapping** keyword was added.

Examples

The following example displays the configured VLANs:

```
ciscoasa# show vlan
10-11,30,40,300
```

The following example displays the secondary VLANs that are mapped to each primary VLAN:

```
ciscoasa# show vlan mapping
Interface                        Secondary VLAN ID                        Mapped VLAN ID
0/1.100                          200                                                 300
0/1.100                          201                                                 300
0/2.500                          400                                                 200
```

Related Commands

Command	Description
clear interface	Clears counters for the **show interface** command.
interface	Configures an interface and enters interface configuration mode.

Command	Description
show interface	Displays the runtime status and statistics of interfaces.

show vm

To display virtual platform information on the ASA virtual, use the show vm command in privileged EXEC mode.

show vm

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

For the ASA virtual, note the following licensing guidelines:

- The number of allowed vCPUs is determined by the vCPU platform license installed.
  - If the number of licensed vCPUs matches the number of provisioned vCPUs, the state is Compliant.
  - If the number of licensed vCPUs is less than the number of provisioned vCPUs, the state is Noncompliant: Over-provisioned.
  - If the number of licensed vCPUs is more than the number of provisioned vCPUs, the state is Compliant: Under-provisioned.
- The memory limit is determined by the number of vCPUs provisioned.
  - If the provisioned memory is at the allowed limit, the state is Compliant.
  - If the provisioned memory is above the allowed limit, the state is Noncompliant: Over-provisioned.
  - If the provisioned memory is below the allowed limit, the state is Compliant: Under-provisioned.
- The Frequency Reservation limit is determined by the number of vCPUs provisioned.
  - If the frequency reservation memory is at or above the required minimum (1000 MHz), the state is Compliant.

- If the frequency reservation memory is below the required minimum (1000 MHz), the state is Compliant: Under-provisioned.

Examples

The following example displays the virtual platform information for an unlicensed ASAv10:

```
ciscoasa# show vm
Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     0
Processor Memory             :     0 MB
Virtual Platform Resource Status
--------------------------------
Number of vCPUs                 :     1     (Noncompliant: Over-provisioned)
Processor Memory                :  2048 MB  (Noncompliant: Over-provisioned)
Hypervisor                      :   VMware
Model Id                        :   ASAv10
```

The following example displays the virtual platform information for a licensed ASAv10:

```
ciscoasa# show vm
Virtual Platform Resource Limits
--------------------------------
Number of vCPUs              :     1
Processor Memory             :  2048 MB
Virtual Platform Resource Status
--------------------------------
Number of vCPUs                 :     1     (Compliant)
Processor Memory                :  2048 MB  (Compliant)
Hypervisor                      :   VMware
Model Id                        :   ASAv10
```

Related Commands

Command	Description
show cpu detail	Shows vCPU information on a per-vCPU basis.

show vni vlan-mapping

To show the mapping between VNI segment IDs and VLAN interfaces or physical interfaces, use the **show vni vlan-mapping** command in privileged EXEC mode.

show vni vlan-mapping

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	—	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

This command is only valid in transparent firewall mode because in routed mode, the mapping between VXLANs and VLANs can include too many values to show.

Examples

See the following output for the **show vni vlan-mapping** command:

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3, interface:
 'g112', vlan 4
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.

Command	Description
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

show vpdn

To show the status of virtual private dial-up network (VPDN) connections such as PPPoE or L2TP, use the **show vpdn** command in privileged EXEC mode.

show vpdn { **group** *name* | **pppinterface** [**id** *number*] | **session** [| **l2tp** | **pppoe**] [**id** *number*] { **packets** | **state** | **window** } | **tunnel** [**l2tp** | **pppoe**] [**id** *number*] { **packets** | **state** | **summary** | **transport** } | **username** *name* }

Syntax Description

group *name*	Shows the VPDN group configuration.
id *number*	(Optional) Shows information about the VPDN session with the specified ID.
l2tp	(Optional) Shows session or tunnel information about L2TP.
packets	Shows session or tunnel packet information.
pppinterface	Shows PPP interface information.
pppoe	(Optional) Show session or tunnel information about PPPoE.
session	Shows session information.
state	Shows session or tunnel state information.
summary	Shows the tunnel summary.
transport	Shows tunnel transport information.
tunnel	Shows tunnel information.
username *name*	Shows user information.
window	Shows session window information.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	We introduced this command.

Usage Guidelines

Use this command to troubleshoot the VPDN PPPoE or L2TP connections.

Examples

The following is sample output from the **show vpdn session** command:

```
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
```

The following is sample output from the **show vpdn tunnel** command:

```
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
```

Related Commands

Command	Description
vpdn group	Configures VPDN client settings

show vpn cluster stats internal

To display the internal counters for VPN clustering, use this command in global configuration or privileged EXEC mode.

show vpn cluster stats internal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.9(1)	Command added.

Related Commands

Command	Description
clear vpn cluster stats internal	Clear all VPN cluster counters.

show vpn load-balancing

To display the runtime statistics for the VPN load-balancing virtual cluster configuration, use the **show vpn-load-balancing** command in global configuration, privileged EXEC, or VPN load-balancing mode.

show vpn load-balancing

Syntax Description

This command has no variables or arguments.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—
Vpn load-balancing	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	Added separate IPsec and SSL columns for both Load (%) display and Session display in the output example.
8.4(2)	New information was added to the displayed output.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **show vpn load-balancing** command displays statistical information for the virtual VPN load-balancing cluster. If the local device is not participating in the VPN load-balancing cluster, this command indicates that VPN load balancing has not been configured for this device.

The asterisk (*) in the output indicates the IP address of the ASA to which you are connected.

Examples

This example displays **show vpn load-balancing** command and its output for a situation in which the local device is participating in the VPN load-balancing cluster:

```
ciscoasa# sh vpn load-balancing
```

```
--------------------------------------------------------------------------
    Status     Role   Failover   Encryption        Cluster IP   Peers
--------------------------------------------------------------------------
   Enabled   Master        n/a     Disabled  192.0.2.255       0
Peers:
--------------------------------------------------------------------------
       Public IP     Role  Pri            Model  Load-Balancing Version
--------------------------------------------------------------------------
  192.0.2.255      Master    5          ASA-5520              3
Total License Load:
--------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials         Other VPN
                   -------------------------------   ---------------------
                        Limit    Used   Load          Limit    Used   Load
--------------------------------------------------------------------------
     192.0.2.255       750       0     0%           750       1     0%
Licenses Used By Inactive Sessions :
--------------------------------------------------------------------------
       Public IP    AnyConnect Premium/Essentials     Inactive Load
--------------------------------------------------------------------------
     192.0.2.255          0               0%
```

On the primary device, the Total License Load output includes information about the primary and backup device; however, the backup device only shows information about itself and not the primary device. Thus, the primary device knows about all licensed members, but the licensed members themselves only know about their own licenses.

The output also contains a License Used by Inactive Session section. When an Secure Client session goes inactive, the ASA keeps that session as long as the session has not terminated by normal means. That way, Secure Client sessions can reconnect using the same webvpn cookie and not have to re-authenticate. The inactive sessions will remain in that state until either the Secure Client resumes the session or an idle timeout occurs. The licenses for those sessions are maintained for these inactive sessions and are represented in this License Used by Inactive Session section.

If the local device is not participating in the VPN load-balancing cluster, the **show vpn load-balancing** command shows a different result:

```
ciscoasa(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

Related Commands

Command	Description
clear configure vpn load-balancing	Removes **vpn load-balancing** command statements from the configuration.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
vpn load-balancing	Enters vpn load-balancing mode.

show vpn-sessiondb

To display information about VPN sessions, use the **show vpn-sessiondb** command in privileged EXEC mode.The command includes options for displaying information in full or in detail, lets you specify type of sessions to display, and provides options to filter and sort the information. The syntax table and usage notes organize the choices accordingly

show vpn-sessiondb [**all**] [**backup** { **index** | **l2l** }] [**detail**] [**ospfv3**] [**failover**] [**full**] [**summary**] [**ratio** { **encryption** | **protocol** }] [**license-summary**] { **anyconnect** | **email-proxy** | **index** *indexnumber* | **l2l** | **ra-ikev1-ipsec** | **ra-ikev2-ipsec** | **vpn-lb** | **webvpn** } [**filter** { **name** *username* | **ipaddress** *IPaddr* | **a-ipaddress** *IPaddr* | **p-ipaddress** *IPaddr* | **tunnel-group** *groupname* | **protocol** *protocol-name* | **encryption** *encryption-algo* | **inactive** }] [**sort** { **name** | **ipaddress** | **a-ipaddress** | **p-ip address** | **tunnel-group** | **protocol** | **encryption** | **inactivity** }]

Syntax Description

all	Displays all clustered sessions, active and backup.
anyconnect	**Displays AnyConnect VPN client sessions, including OSPFv3 session information.**
backup {index | l2l}	Display backup sessions only.
detail	(Optional) Displays extended details about a session. For example, using the detail option for an IPsec session displays additional details such as the IKE hashing algorithm, authentication mode, and rekey interval. If you choose detail, and the full option, the ASA displays the detailed output in a machine-readable format.
email-proxy	(Deprecated) Displays email-proxy sessions.
encryption	Displays the ratio of encryption types as a ratio of the total number of sessions.
failover	Displays the session information for the failover IPsec tunnels.
filter *filter_criteria*	(Optional) Filters the output to display only the information you specify by using one or more of the filter options. For a list of *filter_criteria* options, see the “Usage Guidelines” section.
full	(Optional) Displays streamed, untruncated output. Output is delineated by | characters and a || string between records.
index *indexnumber*	Displays a single session by index number. Specifies the index number for the session, which ranges from 1 - 750.
l2l	Displays VPN LAN-to-LAN session information. When you choose detail, cluster information is also provided.
license-summary	Displays VPN license summary information.
ospfv3	Displays OSPFv3 session information.
protocol	Displays the ratio of protocol types as a ratio of the total number of sessions.

ra-ikev1-ipsec	Displays IPsec IKEv1 sessions.
ra-ikev2-ipsec	Displays details for IKEv2 remote access client connections.
sort *sort_criteria*	(Optional) Sorts the output according to the sort option you specify. For a list of *sort_criteria* options, see the “Usage Guidelines” section.
summary	Displays VPN session summary information.
vpn-lb	Displays VPN load balancing management sessions.
webvpn	Displays clientless SSL VPN sessions, including OSPFv3 session information.

Command Default

There is no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.
8.0(2)	The VLAN field description was added.
8.0(5)	**inactive** as a **filter** option and **inactivity** as a **sort** option were added.
8.2(1)	License information was added to the output.
8.4(1)	The svc keyword was changed to anyconnect. The remote keyword was changed to ra-ikev1-ipsec. The **ratio keyword was added.**
9.0(1)	The **ospfv3** keyword was added, and the OSPFv3 session information is now included in the VPN session summary. The **filter a-ipversion** and **filter p-ipversion** options were added to allow filtering on all Secure Client, LAN-to-LAN, and Clientless SSL VPN sessions assigned IPv4 or IPv6 addresses. Support for multiple context mode was added.
9.1(2)	The failover tunnel type and **failover** keyword to support failover IPsec tunnels was added. See the **failover ipsec pre-shared-key** command.
9.1(4)	Output when using the **detail anyconnect** options and show crypto ipsec sa has been updated to reflect the assigned IPv6 address and to indicate the GRE Transport Mode security association when doing IKEv2 dual traffic.

Release	Modification
9.3(2)	The ra-ikev2-ipsec keyword to display details for IKEv2 remote access client connections was added. The VPN session summary output was updated to include IKEv2 remote access client connections and IKEv2 and IPsec tunnel counts. The VPN licenses usage summary output was updated to add IKEv2 remote access client connections.
9.4(1)	Cert Auth Int and Cert Auth Left were added to the output of this command.
9.8(1)	The email-proxy option was deprecated.
9.9(1)	The all and backup options added.
9.19(1)	The ra-ikev2-ipsec keyword to display both IPv4 and IPv6 addresses assigned to IKEv2 remote access client VPN session.

Usage Guidelines

You can use the following options to filter and to sort the session display:

Filter/Sort Option	Description
filter a-ipaddress *IPaddr*	Filters the output to display information for the specified assigned IP address or addresses only.
sort a-ipaddress	Sorts the display by assigned IP addresses.
filter a-ipversion {v4 | v6}	Filters the output to display information about all Secure Client sessions assigned IPv4 or IPv6 addresses.
filter encryption *encryption-algo*	Filters the output to display information for sessions using the specified encryption algorithm(s) only.
sort encryption	Sorts the display by encryption algorithm. Encryption algorithms include: aes128, aes192, aes256, des, 3des, rc4
filter inactive	Filters inactive sessions which have gone idle and have possibly lost connectivity (due to hibernation, mobile device disconnection, and so on). The number of inactive sessions increases when TCP keepalives are sent from the ASA without a response from the Secure Client. Each session is time stamped with the SSL tunnel drop time. If the session is actively passing traffic over the SSL tunnel, 00:00m:00s is displayed. **Note** The ASA does not send TCP keepalives to some devices (such as the iPhone, iPad, and iPod) to save battery life, so the failure detection cannot distinguish between a disconnect and a sleep. For this reason, the inactivity counter remains as 00:00:00 by design.
sort inactivity	Sorts inactive sessions.
filter ipaddress *IPaddr*	Filters the output to display information for the specified inside IP address or addresses only.
sort ipaddress	Sorts the display by inside IP addresses.

Filter/Sort Option	Description
filter name *username* **sort name**	Filters the output to display sessions for the specified username(s). Sorts the display by usernames in alphabetical order.
filter p-address *IPaddr*	Filters the output to display information for the specified outside IP address only.
sort p-address	Sorts the display by the specified outside IP address or addresses.
filter p-ipversion {v4 | v6}	Filters the output to display information about all Secure Client sessions originating from endpoints with IPv4 or IPv6 addresses.
filter protocol *protocol-name*	Filters the output to display information for sessions using the specified protocol(s) only.
sort protocol	Sorts the display by protocol. Protocols include: IKE, IMAP4S, IPsec, IPsecLAN2LAN, IPsecLAN2LANOverNatT, IPsecOverNatT, IPsecoverTCP, IPsecOverUDP, SMTPS, userHTTPS, vcaLAN2LAN
filter tunnel-group *groupname*	Filters the output to display information for the specified tunnel group(s) only.
sort tunnel-group	Sorts the display by tunnel group.
|	Modifies the output, using the following arguments: {begin | include | exclude | grep | [-v]} {reg_exp}

Note: The command output shows the username only up to 120 characters. If the length exceeds 120, the remaining characters are truncated and displayed in the command output.

Examples

The following is sample output from the **show vpn-sessiondb** command:

```
ciscoasa
#
 show vpn-sessiondb
---------------------------------------------------------------------------
VPN Session Summary
---------------------------------------------------------------------------
                               Active : Cumulative : Peak Concur : Inactive
                             ----------------------------------------------
AnyConnect Client            :      1 :         78 :           2 :        0
  SSL/TLS/DTLS               :      1 :         72 :           2 :        0
  IKEv2 IPsec                :      0 :          6 :           1 :        0
IKEv2 Generic IPsec Client   :      0 :          0 :           0
Clientless VPN               :      0 :          8 :           2
  Browser                    :      0 :          8 :           2
---------------------------------------------------------------------------
Total Active and Inactive    :      1             Total Cumulative :     86
Device Total VPN Capacity    :    750
Device Load                  :     0%
---------------------------------------------------------------------------
---------------------------------------------------------------------------
Tunnels Summary
---------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                             ---------------------------------------------
IKEv2                        :      0 :          6 :             1
IPsecOverNatT                :      0 :          6 :             1
Clientless                   :      0 :         17 :             2
AnyConnect-Parent            :      1 :         69 :             2
SSL-Tunnel                   :      1 :         75 :             2
DTLS-Tunnel                  :      1 :         56 :             2
----------------------------------------------------------------------------
Totals                       :      3 :        229
----------------------------------------------------------------------------
----------------------------------------------------------------------------
IPv6 Usage Summary
----------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                             ---------------------------------------------
AnyConnect SSL/TLS/DTLS      :        :            :
  IPv6 Peer                  :      1 :         41 :           2
  Tunneled IPv6              :      1 :         70 :           2
AnyConnect IKEv2             :        :            :
  IPv6 Peer                  :      0 :          4 :           1
Clientless                   :        :            :
  IPv6 Peer                  :      0 :          1 :           1
----------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb detail l2l** command, showing detailed information about LAN-to-LAN sessions:

```
ciscoasa
#
 show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.0
Index        : 1
IP Addr      : 172.16.0.0
Protocol     : IKEv2 IPsec
Encryption   : IKEv2: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 240                    Bytes Rx     : 160
Login Time   : 14:50:35 UTC Tue May 1 2012
Duration     : 0h:00m:11s
IKEv2 Tunnels: 1
IPsec Tunnels: 1
IKEv2:
  Tunnel ID    : 1.1
  UDP Src Port : 500                    UDP Dst Port : 500
  Rem Auth Mode: preSharedKeys
  Loc Auth Mode: preSharedKeys
  Encryption   : AES256                 Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86389 Seconds
  PRF          : SHA1                   D/H Group    : 5
  Filter Name  :
  IPv6 Filter  :
IPsec:
  Tunnel ID    : 1.2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                 Hashing      : SHA1
  Encapsulation: Tunnel                 PFS Group    : 5
  Rekey Int (T): 120 Seconds            Rekey Left(T): 107 Seconds
  Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4608000 K-Bytes
  Idle Time Out: 30 Minutes             Idle TO Left : 29 Minutes
  Bytes Tx     : 240                    Bytes Rx     : 160
  Pkts Tx      : 3                      Pkts Rx      : 2
```

```
NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 13 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
The following is sample output from the show vpn-sessiondb detail index 1
 command:
AsaNacDev# show vpn-sessiondb detail index 1
Session Type: Remote Detailed
Username     : user1
Index        : 1
Assigned IP  : 192.168.2.70           Public IP    : 10.86.5.114
Protocol     : IPsec                  Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                      Bytes Rx     : 604533
Client Type  : WinNT                  Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy
VM Result    : Static
VLAN         : 10
IKE Sessions: 1 IPsec Sessions: 1 NAC Sessions: 1
IKE:
  Session ID   : 1
  UDP Src Port : 500                    UDP Dst Port : 500
  IKE Neg Mode : Aggressive             Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                   Hashing      : MD5
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 61078 Seconds
  D/H Group    : 2
IPsec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                 Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds          Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                      Bytes Rx     : 604533
  Pkts Tx      : 0                      Pkts Rx      : 8126
NAC:
  Reval Int (T): 3000 Seconds           Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds            EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds              Posture Token: Healthy
  Redirect URL : www.cisco.com
```

The following is sample output from the **show vpn-sessiondb ospfv3** command:

```
asa# show vpn-sessiondb ospfv3

Session Type: OSPFv3 IPsec
Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:13m:11s
```

The following is sample output from the **show vpn-sessiondb detail ospfv3** command:

```
asa# show vpn-sessiondb detail ospfv3
```

```
Session Type: OSPFv3 IPsec Detailed
Connection   :
Index        : 1                      IP Addr      : 0.0.0.0
Protocol     : IPsec
Encryption   : IPsec: (1)none         Hashing      : IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 0
Login Time   : 15:06:41 EST Wed Feb 1 2012
Duration     : 1d 5h:14m:28s
IPsec Tunnels: 1
IPsec:
  Tunnel ID    : 1.1
  Local Addr   : ::/0/89/0
  Remote Addr  : ::/0/89/0
  Encryption   : none                   Hashing      : SHA1
  Encapsulation: Transport
  Idle Time Out: 0 Minutes              Idle TO Left : 0 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 0
  Pkts Tx      : 0                      Pkts Rx      : 0

NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 105268 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

The following is sample output from the **show vpn-sessiondb summary** command:

```
ciscoasa# show vpn-sessiondb summary

---------------------------------------------------------------------------
VPN Session Summary
---------------------------------------------------------------------------
                               Active : Cumulative : Peak Concur : Inactive
                             ----------------------------------------------
OSPFv3 IPsec                 :      1 :          1 :           1
---------------------------------------------------------------------------
Total Active and Inactive    :      1            Total Cumulative :      1
Device Total VPN Capacity    :  10000
Device Load                  :     0%
-----------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb summary** command for generic IKEv2 IPsec remote access sessions:

```
ciscoasa# show vpn-sessiondb summary
---------------------------------------------------------------------------
VPN Session Summary
---------------------------------------------------------------------------
                               Active : Cumulative : Peak Concur : Inactive
                             ----------------------------------------------
Generic IKEv2 Remote Access  :      1 :          1 :           1
---------------------------------------------------------------------------
Total Active and Inactive    :      1            Total Cumulative :      1
Device Total VPN Capacity    :    250
Device Load                  :     0%
---------------------------------------------------------------------------
---------------------------------------------------------------------------
Tunnels Summary
---------------------------------------------------------------------------
                               Active : Cumulative : Peak Concurrent
                             ----------------------------------------------
IKEv2                        :      1 :          1 :               1
```

```
IPsec                        :      1 :          1 :              1
---------------------------------------------------------------------------
Totals                       :      2 :          2
---------------------------------------------------------------------------
```

The following is sample output from the **show vpn-sessiondb det anyconnect** command:

```
ciscoasa# show vpn-sessiondb det anyconnect
Session Type: AnyConnect Detailed
Username     : userab                 Index        : 2
Assigned IP  : 65.2.1.100             Public IP    : 75.2.1.60
Assigned IPv6: 2001:1000::10
Protocol     : IKEv2 IPsecOverNatT AnyConnect-Parent
License      : AnyConnect Premium
Encryption   : IKEv2: (1)3DES  IPsecOverNatT: (1)3DES  AnyConnect-Parent: (1)none
Hashing      : IKEv2: (1)SHA1  IPsecOverNatT: (1)SHA1  AnyConnect-Parent: (1)none
Bytes Tx     : 0                      Bytes Rx     : 21248
Pkts Tx      : 0                      Pkts Rx      : 238
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : test1
Login Time   : 22:44:59 EST Tue Aug 13 2013
Duration     : 0h:02m:42s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1
AnyConnect-Parent:
  Tunnel ID    : 2.1
  Public IP    : 75.2.1.60
  Encryption   : none                   Hashing      : none
  Auth Mode    : userPassword
  Idle Time Out: 400 Minutes            Idle TO Left : 397 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Client OS    : Windows
  Client Type  : AnyConnect
  Client Ver   : 3.1.05050
IKEv2:
  Tunnel ID    : 2.2
  UDP Src Port : 64251                  UDP Dst Port : 4500
  Rem Auth Mode: userPassword
  Loc Auth Mode: rsaCertificate
  Encryption   : 3DES                   Hashing      : SHA1
  Rekey Int (T): 86400 Seconds          Rekey Left(T): 86241 Seconds
  PRF          : SHA1                   D/H Group    : 2
  Filter Name  : mixed1
  Client OS    : Windows
IPsecOverNatT:
  Tunnel ID    : 2.3
  Local Addr   : 75.2.1.23/255.255.255.255/47/0
  Remote Addr  : 75.2.1.60/255.255.255.255/47/0
  Encryption   : 3DES                   Hashing      : SHA1
  Encapsulation: Transport, GRE
  Rekey Int (T): 28400 Seconds          Rekey Left(T): 28241 Seconds
  Idle Time Out: 400 Minutes            Idle TO Left : 400 Minutes
  Conn Time Out: 500 Minutes            Conn TO Left : 497 Minutes
  Bytes Tx     : 0                      Bytes Rx     : 21326
  Pkts Tx      : 0                      Pkts Rx      : 239
NAC:
  Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds              EoU Age(T)   : 165 Seconds
  Hold Left (T): 0 Seconds              Posture Token:
  Redirect URL :
```

```
Output from show vpn-sessiondb detail anyconnect showing a DTLS tunnel.
...
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10280                  Bytes Rx     : 3819
Pkts Tx      : 8                      Pkts Rx      : 45
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : DfltGrpPolicy          Tunnel Group : DefaultWEBVPNGroup
Login Time   : 09:42:39 UTC Tue Dec 5 2017
Duration     : 0h:00m:07s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 000000000000010005a266a0f
Security Grp : none
...
DTLS-Tunnel:
  Tunnel ID    : 1.3
  Assigned IP  : 95.0.225.240           Public IP    : 85.0.224.13
  Encryption   : AES256                 Hashing      : SHA1
  Ciphersuite  : AES256-SHA
  Encapsulation: DTLSv1.2             UDP Src Port : 51008
  UDP Dst Port : 443                    Auth Mode    : userPassword
  Idle Time Out: 30 Minutes             Idle TO Left : 30 Minutes
  Client OS    : Windows
  Client Type  : DTLS VPN Client
  Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.x
```

The following example is sample output from the **show vpn-sessiondb ra-ikev2-ipsec** command:

```
ciscoasa(config)# show vpn-sessiondb detail ra-ikev2-ipsec
Session Type: Generic Remote-Access IKEv2 IPsec Detailed
Username     : IKEV2TG                Index        : 1
Assigned IP  : 95.0.225.200           Public IP    : 85.0.224.12
Assigned IPv6: 2001:db8::1
Protocol     : IKEv2 IPsec
License      : AnyConnect Essentials
Encryption   : IKEv2: (1)3DES  IPsec: (1)AES256
Hashing      : IKEv2: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 0                      Bytes Rx     : 17844
Pkts Tx      : 0                      Pkts Rx      : 230
Pkts Tx Drop : 0                      Pkts Rx Drop : 0
Group Policy : GroupPolicy_IKEV2TG    Tunnel Group : IKEV2TG
Login Time   : 11:39:54 UTC Tue May 6 2014
Duration     : 0h:03m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 5f00e105000010005368ca0a
Security Grp : none
IKEv2 Tunnels: 1
IPsec Tunnels: 1
```

The following is sample output from the **show vpn-sessiondb license-summary** command:

```
---------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
---------------------------------------------------------------------------
                                     Status : Capacity : Installed :  Limit
                                  -----------------------------------------
AnyConnect Premium               : DISABLED :      250 :        10 :   NONE
AnyConnect Essentials            :  ENABLED :      250 :       250 :   NONE
Other VPN (Available by Default) :  ENABLED :      250 :       250 :   NONE
```

```
Shared License Server            : DISABLED
Shared License Participant       : DISABLED
AnyConnect for Mobile            : DISABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     : DISABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   : DISABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
---------------------------------------------------------------------------
---------------------------------------------------------------------------
VPN Licenses Usage Summary
---------------------------------------------------------------------------
                          Local : Shared :   All   :   Peak :  Eff.  :
                         In Use : In Use : In Use : In Use :  Limit : Usage
                        ---------------------------------------------------
AnyConnect Essentials  :      1 :      0 :      1 :      1 :    250 :    0%
  AnyConnect Client    :                 :      0 :      0          :    0%
    AnyConnect Mobile  :                 :      0 :      0          :    0%
  Generic IKEv2 Client :                 :      1 :      1          :    0%
Other VPN              :                 :      0 :      0 :    250 :    0%
  Cisco VPN Client     :                 :      0 :      0          :    0%
---------------------------------------------------------------------------
Shared License Network Summary
---------------------------------------------------------------------------
AnyConnect Premium
  Total shared licenses in network                                    : 500
  Shared licenses held by this participant                            :  0
  Shared licenses held by all participants in the network             :  0
---------------------------------------------------------------------------
```

As shown in the examples, the fields displayed in response to the **show vpn-sessiondb** command vary, depending on the keywords you enter. Table 14-2 describes these fields.

Table 96: show vpn-sessiondb Command Fields

Field	Description
Auth Mode	Protocol or mode used to authenticate this session.
Assigned IP	Private IP address assigned to the remote client for current session.
Assigned IPv6	Private IPv6 address assigned to the remote client for current session.
Bytes Rx	Total number of bytes received from the remote peer or client by the ASA.
Bytes Tx	Number of bytes transmitted to the remote peer or client by the ASA.
Client Type	Client software running on the remote peer, if available.
Client Ver	Version of the client software running on the remote peer.
Connection	Name of the connection or the private IP address.
D/H Group	Diffie-Hellman Group. The algorithm and key size used to generate IPsec SA encryption keys.
Duration	Elapsed time (HH:MM:SS) between the session login time and the last screen refresh.
EAPoUDP Session Age	Number of seconds since the last successful posture validation.

Field	Description
Encapsulation	Mode used to apply IPsec ESP (Encapsulation Security Payload protocol) encryption and authentication (that is, the part of the original IP packet that has ESP applied).
Encryption	Data encryption algorithm this session is using, if any.
EoU Age (T)	EAPoUDP Session Age. Number of seconds since the last successful posture validation.
Filter Name	Username specified to restrict the display of session information.
Hashing	Algorithm used to create a hash of the packet, which is used for IPsec data authentication.
Hold Left (T)	Hold-Off Time Remaining. 0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
Hold-Off Time Remaining	0 seconds if the last posture validation was successful. Otherwise, the number of seconds remaining before the next posture validation attempt.
IKE Neg Mode	IKE (IPsec Phase 1) mode for exchanging key information and setting up SAs: Aggressive or Main.
IKE Sessions	Number of IKE (IPsec Phase 1) sessions; usually 1. These sessions establish the tunnel for IPsec traffic.
Index	Unique identifier for this record.
IP Addr	Private IP address assigned to the remote client for this session. This is also known as the “inner” or “virtual” IP address. It lets the client appear to be a host on the private network.
IPsec Sessions	Number of IPsec (Phase 2) sessions, which are data traffic sessions through the tunnel. Each IPsec remote-access session can have two IPsec sessions: one consisting of the tunnel endpoints, and one consisting of the private networks reachable through the tunnel.
License Information	Shows information about the shared SSL VPN license.
Local IP Addr	IP address assigned to the local endpoint of the tunnel (that is the interface on the ASA).
Login Time	Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.

Field	Description
NAC Result	State of Network Admission Control Posture Validation. It can be one of the following: • Accepted—The ACS successfully validated the posture of the remote host. • Rejected—The ACS could not successfully validate the posture of the remote host. • Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the ASA. • Non-Responsive—The remote host did not respond to the EAPoUDP Hello message. • Hold-off—The ASA lost EAPoUDP communication with the remote host after successful posture validation. • N/A—NAC is disabled for the remote host according to the VPN NAC group policy. • Unknown—Posture validation is in progress.
NAC Sessions	Number of Network Admission Control (EAPoUDP) sessions.
Packets Rx	Number of packets received from the remote peer by the ASA.
Packets Tx	Number of packets transmitted to the remote peer by the ASA.
PFS Group	Perfect Forward Secrecy group number.
Posture Token	Informational text string configurable on the Access Control Server. The ACS downloads the posture token to the ASA for informational purposes to aid in system monitoring, reporting, debugging, and logging. A typical posture token is Healthy, Checkup, Quarantine, Infected, or Unknown.
Protocol	Protocol the session is using.
Public IP	Publicly routable IP address assigned to the client.
Redirect URL	Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the ASA. The Redirect URL is an optional part of the access policy payload. The ASA redirects all HTTP (port 80) and HTTPS (port 443) requests for the remote host to the Redirect URL if it is present. If the access policy does not contain a Redirect URL, the ASA does not redirect HTTP and HTTPS requests from the remote host. Redirect URLs remain in force until either the IPsec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.
Rekey Int (T or D)	Lifetime of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.

Field	Description
Rekey Left (T or D)	Lifetime remaining of the IPsec (IKE) SA encryption keys. The T value is the lifetime in duration, the D value is in data transmitted. Only the T value is shown for remote access VPN.
Rekey Time Interval	Lifetime of the IPsec (IKE) SA encryption keys.
Remote IP Addr	IP address assigned to the remote endpoint of the tunnel (that is the interface on the remote peer).
Reval Int (T)	Revalidation Time Interval. Interval in seconds required between each successful posture validation.
Reval Left (T)	Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Revalidation Time Interval	Interval in seconds required between each successful posture validation.
Session ID	Identifier for the session component (subsession). Each SA has its own identifier.
Session Type	Type of session: LAN-to-LAN or Remote
SQ Int (T)	Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the ASA to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Status Query Time Interval	Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the ASA to the remote host to indicate whether the host has experienced any changes in posture since the last posture validation.
Time Until Next Revalidation	0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Tunnel Group	Name of the tunnel group referenced by this tunnel for attribute values.
UDP Dst Port or UDP Destination Port	Port number used by the remote peer for UDP.
UDP Src Port or UDP Source Port	Port number used by the ASA for UDP.
Username	User login name with which the session is established.
VLAN	Egress VLAN interface assigned to this session. The ASA forwards all traffic to that VLAN. One of the following elements specifies the value: • Group policy • Inherited group policy

Related Commands

Command	Description
show running-configuration vpn-sessiondb	Displays the VPN session database running configuration (max-other-vpn-limit, max-anyconnect-premium-or-essentials-limit).
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show vpn-sessiondb ratio

To display the ratio of current sessions as a percentage by protocol or encryption algorithm, use the **show vpn-sessiondb ratio** command in privileged EXEC mode.

show vpn-sessiondb ratio { **protocol | encryption** } [**filter** *groupname*]

Syntax Description

encryption	Identifies the encryption protocols you want to display. Refers to phase 2 encryption. Encryption algorithms include:	
	aes128	des
	aes192	3des
	aes256	rc4
filter *groupname*	Filters the output to include session ratios only for the tunnel group you specify.	
protocol	Identifies the protocols you want to display. Protocols include:	
	IKEv1	L2TPOverIPsecOverNatT
	IKEv2	Clientless
	IPsec	Port-Forwarding
	IPsecLAN2LAN	IMAP4S
	IPsecLAN2LANOverNatT	POP3S
	IPsecOverNatT	SMTPS
	IPsecOverTCP	AnyConnect-Parent
	IPsecOverUDP	SSL-Tunnel
	L2TPOverIPsec	DTLS-Tunnel

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The output was enhanced to include IKEv2.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output for the **show vpn-sessiondb ratio** command, with **encryption** as the argument:

```
ciscoasa# show vpn-sessiondb ratio encryption
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9
Encryption                Sessions       Percent
none                      0               0%
DES                       1              20%
3DES                      0               0%
AES128                    4          80%
AES192                    0               0%
AES256                    0               0%
```

The following is sample output for the **show vpn-sessiondb ratio** command with **protocol** as the argument:

```
ciscoasa# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10
Protocol                  Sessions       Percent
IKE                       0               0%
IPsec                     1              20%
IPsecLAN2LAN              0               0%
IPsecLAN2LANOverNatT      0               0%
IPsecOverNatT             0               0%
IPsecOverTCP              1        20%
IPsecOverUDP              0               0%
L2TP                      0               0%
L2TPOverIPsec             0               0%
L2TPOverIPsecOverNatT     0               0%
PPPoE                     0               0%
vpnLoadBalanceMgmt        0               0%
userHTTPS                 0               0%
IMAP4S                    3      30%
POP3S                     0               0%
SMTPS                     3        30%
```

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb summary	Displays a session summary, including total current session, current sessions of each type, peak and total cumulative, maximum concurrent sessions

show vpn-sessiondb summary

To display the number of IPsec, Cisco Secure Client, and NAC sessions, use the **show vpn-sessiondb summary** command in privileged EXEC mode.

show vpn-sessiondb summary

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	—	• Yes	• Yes

Command History

Release	Modification
7.0(7)	This command was added.
8.0(2)	The VLAN Mapping Sessions table was added.
8.0(5)	New output for active, cumulative, peak concurrent, and inactive was added.
9.0(1)	Support for multiple context mode was added.

Examples

The following is sample output for the **show vpn-sessiondb summary** command with one IPsec IKEv1 and one clientless session:

Note A device in standby does not differentiate active from inactive sessions.

```
ciscoasa# show vpn-sessiondb summary
VPN Session Summary
Sessions:
       Active : Cumulative : Peak Concurrent : Inactive :
 Clientless VPN        :  1:   2:    1  Browser       :  1:   2:    1 IKEv1 IPsec/L2TP IPsec
     0  :  1:   1:    1
Total Active and Inactive: 2          Total Cumulative: 3
Device Total VPN Capacity: 10000
Device Load      : 0%
License Information:
 Shared VPN License Information:
  SSL VPN        : 12000
   Allocated to this device       :  0
   Allocated to network       :  0
   Device limit       : 750
IPsec   : 750   Configured : 750    Active :  0   Load :  0%
SSL VPN  : 750  Configured : 750    Active :   0  Load :  0%
      Active : Cumulative : Peak Concurrent
SSL VPN     :   0 :   1 :    1
Totals    :   0 :   1 :
Active NAC Sessions:
  Accepted                : 0
  Rejected                : 0
  Exempted                : 0
  Non-responsive          : 0
Hold-off                : 0
  N/A                     : 0
Active VLAN Mapping Sessions:
  Static                  : 0
  Auth                    : 0
  Access                  : 0
  Guest                   : 0
  Quarantine              : 0
  N/A                     : 0
ciscoasa#
```

You can use the SSL output to determine the physical device resources in respect to the number of licenses. A single user session may occupy a license but could use multiple tunnels. For example, an Secure Client user with DTLS often has the parent session, SSL tunnel, and DTLS tunnels associated with it.

Note The parent session represents when the client is not actively connected. It does not represent an encrypted tunnel. If the client shuts down, or sleeps, IPsec, IKE, TLS, and DLTLS tunnels are closed, but the parent session remains until the idle time or maximum connect time limit is reached. This enables the user to reconnect without reauthenticating.

With this example, you would see three tunnels allocated on the device, even if only one user is logged in. An IPsec LAN-to-LAN tunnel counts as one session, and it allows many host-to-host connections through the tunnel. An IPsec remote access session is one remote access tunnel that supports one user connection.

From the output you can see which sessions are active. If a session has no underlying tunnels associated to it, the status is *waiting to resume* mode (displayed as clientless in the session output). This mode means that dead peer detection from the head-end device has started, and the head-end device can no longer communicate with the client. When you encounter this condition, you can hold the session to allow the user to roam networks, go to sleep, recover the session, and so on. These sessions count towards the actively connected sessions (from a license standpoint) and are cleared with a user idle timeout, a user logging out, or a resumption of the original session.

The Active SSL VPN With Client column shows the number of active connections passing data. The Cumulative SSL VPN With Client column shows the number of active sessions that have been established. It includes those that are inactive and increments only when a new session is added. The Peak Concurrent SSL VPN With Client column shows the peak number of concurrently active sessions that are passing data. The Inactive SSL VPN With Client column shows how long the Secure Client was disconnected. You can use this Inactivity timeout value to determine when licenses are expired. The ASA can then determine whether reconnection is possible. These are Secure Client sessions without an active SSL tunnel associated with them.

Table 14-3 explains the fields in the Active Sessions and Session Information tables.

Table 97: show vpn-sessiondb summary Command: Active Sessions and Session Information Fields

Field	Description
Concurrent Limit	Maximum number of concurrently active sessions permitted on this ASA.
Cumulative Sessions	Number of sessions of all types since the ASA was last booted or reset.
LAN-to-LAN	Number of IPsec LAN-to-LAN sessions that are currently active.
Peak Concurrent	Highest number of sessions of all types that were concurrently valid sessions (active + inactive) since the ASA was last booted or reset.
Percent Session Load	Percentage of the vpn session allocation in use. This value equals the Total Active Sessions divided by the maximum number of sessions available, displayed as a percentage. The maximum number of sessions available can be either of the following: • Maximum number of IPsec and SSL VPN sessions licensed • **vpn-sessiondb ?** (maximum number of sessions configured) • **max-anyconnect-premium-or-essentials-limit** (maximum AnyConnect Premium or Essentials session limit) • **max-other-vpn-limit** (maximum other VPN session limit)
Remote Access	ra-ikev1-ipsec—Number of IKEv1 IPsec remote-access user, L2TP over IPsec, and IPsec through NAT sessions that are currently active.
Total Active Sessions	Number of sessions of all types that are currently active.

Examples

The Active NAC Sessions table shows general statistics about remote peers that are subject to posture validation.

The Cumulative NAC Sessions table shows general statistics about remote peers that are or have been subject to posture validation.

Table 14-2 explains the fields in the Active NAC Sessions and Total Cumulative NAC Sessions tables.

Table 98: show vpn-sessiondb summary Command: Active NAC Sessions and Total Cumulative NAC Sessions Fields

Field	Description
Accepted	Number of peers that passed posture validation and have been granted an access policy by an Access Control Server.
Exempted	Number of peers that are not subject to posture validation because they match an entry in the Posture Validation Exception list configured on the ASA.
Hold-off	Number of peers for which the ASA lost EAPoUDP communications after a successful posture validation. The NAC Hold Timer attribute (Configuration > VPN > NAC) determines the delay between this type of event and the next posture validation attempt for each peer.
N/A	Number of peers for which NAC is disabled according to the VPN NAC group policy.

Field	Description
Non-responsive	Number of peers not responsive to Extensible Authentication Protocol (EAP) over UDP requests for posture validation. Peers on which no CTA is running do not respond to these requests. If the ASA configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the ASA for these peers. Otherwise, the ASA assigns the NAC default policy.
Rejected	Number of peers that failed posture validation or were not granted an access policy by an Access Control Server.

The Active VLAN Mapping Sessions table shows general statistics about remote peers that are subject to posture validation.

The Cumulative VLAN Mapping Sessions table shows general statistics about remote peers that are or have been subject to posture validation.

Table 14-5 explains the fields in the Active VLAN Mapping Sessions and Cumulative VLAN Mapping Sessions tables.

Table 99: show vpn-sessiondb summary Command: Active VLAN Mapping Sessions and Cumulative Active VLAN Mapping Sessions Fields

Field	Description
Access	Reserved for future use.
Auth	Reserved for future use.
Guest	Reserved for future use.
N/A	Reserved for future use.
Quarantine	Reserved for future use.
Static	This field shows the number of VPN sessions assigned to a pre-configured VLAN.

Related Commands

Command	Description
show vpn-sessiondb	Displays sessions with or without extended details, optionally filtered and sorted by criteria you specify.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.

show wccp

To display global statistics related to Web Cache Communication Protocol (WCCP), use the **show wccp** command in privileged EXEC mode.

show wccp { **web-cache |** *service-number* } [*detail* | *view*]

Syntax Description

detail	(Optional) Displays information about the router and all web caches.
service-number	(Optional) Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 256. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99.
view	(Optional) Displays other members of a particular service group have or have not been detected.
web-cache	Specifies statistics for the web-cache service.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to display WCCP information:

```
ciscoasa(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0
    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
ciscoasa(config)#
```

Related Commands

Commands	Description
wccp	Enables support of WCCP with service groups.
wccp redirect	Enables support of WCCP redirection.

show webvpn anyconnect

To view information about SSL VPN client images installed on the ASA and loaded in cache memory, or to test a file to see if it is a valid client image, use the show webvpn anyconnect command from privileged EXEC mode.

show webvpn anyconnect [**image** *filename*]

Syntax Description

image *filename*	Specifies the name of a file to test as an SSL VPN client image file.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
8.4(1)	The **show webvpn** anyconnect form of the command replaced show webvpn svc.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Use the **show webvpn anyconnect** command to view information about SSL VPN client images that are loaded in cache memory and available for download to remote PCs. Use the **image** *filename* keyword and argument to test a file to see if it is a valid image. If the file is not a valid image, the following message appears:

```
ERROR: This is not a valid SSL VPN Client image file.
```

Examples

The following example shows the output of the show webvpn anyconnect command for currently installed images:

```
ciscoasa# show webvpn anyconnect
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 2
```

```
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

The following example shows the output of the **show webvpn anyconnect image** *filename* command for a valid image:

```
ciscoasa(config-webvpn)# show webvpn anyconnect image sslclient-win-1.0.2.127.pkg
This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

Related Commands

Command	Description
anyconnect enable	Enables the ASA to download the SSL VPN client to remote PCs.
anyconnect image	Causes the security appliance to load SSL VPN client files from flash memory to cache memory, and specifies the order in which the security appliance downloads portions of the client image to the remote PC as it attempts to match the client image with the operating system.
vpn-tunnel-protocol	Enables specific VPN tunnel protocols for remote VPN users, including SSL used by an SSL VPN client.

show webvpn anyconnect external-browser-pkg

To view information about the single sing-on external browser package file, use the show webvpn anyconnect external-browser-pkg command from privileged EXEC mode.

show webvpn anyconnect external-browser-pkg [*package-path*]

Syntax Description

package-path	Specifies the path where the AnyConnect external browser package is installed.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.17(1)	This command was added.

Usage Guidelines

Use the **show webvpn anyconnectexternal-browser-pkg** command to view information about the AnyConnect external browser package. Use the *package-path* keyword and argument to specify the path where the package is installed.

Examples

The following example shows the output of the show webvpn anyconnect external-browser-pkg command:

```
ciscoasa# show webvpn anyconnect external-browser-pkg
disk0:/external-sso-98.161.00015-webdeploy-k9.pkg
Cisco AnyConnect External Browser Headend Package
  98.161.00015
  Wed 07/15/21 15:49:27.81738
```

Related Commands

Command	Description
anyconnect image	Causes the security appliance to load SSL VPN client files from flash memory to cache memory, and specifies the order in which the security appliance downloads portions of the client image to the remote PC as it attempts to match the client image with the operating system.
external-browser	Configures the default operating system for single sign-on authentication.

show webvpn csd (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To determine whether CSD is enabled, display the CSD version in the running configuration, determine what image is providing the Host Scan package, and to test a file to see if it is a valid CSD distribution package, use the show webvpn csd command in privileged EXEC mode.

show webvpn csd [**image** *filename*]

Syntax Description

filename	Specifies the name of a file to test for validity as a CSD distribution package. It must take the form **csd_n.n.n-k9.pkg**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated. It is replaced by **show webvpn hostscan**.
9.0(1)	Support for multiple context mode was added.

Examples

Use the **show webvpn csd** command to check the operational status of CSD. The CLI responds with a message indicating if CSD is installed and if it is enabled, if Host Scan is installed and if it is enabled, and which image is supplying the Host Scan package if there is both a CSD package and a Host Scan package installed.

```
ciscoasa# show webvpn csd
```

These are the messages you could receive:

- Secure Desktop is not installed

Hostscan is not installed

- Secure Desktop version n.n.n.n is currently installed but not enabled

Standalone Hostscan package is not installed (Hostscan is currently installed via the CSD package but not enabled)

- Secure Desktop version n.n.n.n is currently installed and enabled

```
Standalone Hostscan package is not installed (Hostscan is currently installed and enabled
via the CSD package)
```

The message, “ Secure Desktop version n.n.n.n is currently installed ... ” means that the image is loaded on the ASA and in the running configuration. The image can be either enabled or not enabled. You can go to webvpn configuration mode and enter the **csd enable** command to enable CSD.

The messaage, “ (Hostscan is currently installed and enabled via the CSD package) ” means that the Host Scan package delivered with the CSD package is the Host Scan package in use.

- Secure Desktop version n.n.n.n is currently installed and enabled

Hostscan version n.n.n.n is currently installed and enabled

The message, “ Secure Desktop version n.n.n.n is currently installed and enabled Hostscan version n.n.n.n is currently installed and enabled ” means that both CSD and a Host Scan package, delivered either as a standalone package or as part of an Secure Client image, are installed. If Host Scan is enabled and both CSD and an Secure Client image with Host Scan, or a standalone Host Scan package, are installed and enabled, the Host Scan package delivered as a standalone package or as part of an Secure Client image takes precedence over the one provided with a CSD package.

- Secure Desktop version n.n.n.n is currently installed but not enabled

Hostscan version n.n.n.n is currently installed but not enabled

Use the **show webvpn csd image** *filename* command to test a file to determine if a CSD distribution package is valid.

ciscoasa# **show webvpn csd image csd_n.n.n-k9.pkg**

The CLI responds with one of the following messages when you enter this command:

- ERROR: This is not a valid Secure Desktop image file.

Make sure the filename is in the form the form **csd_n.n.n_k9.pkg**. If the csd package does not have this naming convention, replace the file with one obtained from the following website:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

Then reenter the **show webvpn csd image** command. If the image is valid, use the **csd image** and **csd enable** commands in webvpn configuration mode to install and enable CSD.

- This is a valid Cisco Secure Desktop image:

Version : 3.6.172.0

Hostscan Version : 3.6.172.0

Built on : Wed Feb 23 15:46:44 MST 2011

Note that the CLI provides both the version and date stamp if the file is valid.

Related Commands

Command	Description
csd enable	Enables CSD for management and remote user access.
csd image	Copies the CSD image named in the command, from the flash drive specified in the path to the running configuration.

show webvpn debug-condition

To view information about the WebVPN debug filters, use the **show webvpn debug-condition** command from privileged EXEC mode.

show webvpn debug-condition

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn debug-condition** command.

Example

The following example displays information about the webvpn debug filters:

```
ciscoasa#show webvpn debug-condition
INFO: Webvpn conditional debug is turned OFF
```

show webvpn group-alias

To display the aliases for a specific tunnel-group or for all tunnel groups, use the **group-alias** command in privileged EXEC mode.

show webvpn group-alias [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the group aliases.

Command Default

If you do not enter a tunnel-group name, this command displays all the aliases for all the tunnel groups.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1	This command was added.
9.0	Support for multiple context mode was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn group-alias** command.

Each tunnel group can have multiple aliases or no alias.

Examples

The following example shows the **show webvpn group-alias** command that displays the aliases for the tunnel group “devtest” and the output of that command:

```
ciscoasa# show webvpn group-alias devtest
QA
Fra-QA
```

Related Commands

Command	Description
group-alias	Specifies one or more URLs for the group.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn group-url

To display the URLs for a specific tunnel-group or for all tunnel groups, use the **group-url** command in privileged EXEC mode.

show webvpn group-url [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the URLs.

Command Default

If you do not enter a tunnel-group name, this command displays all the URLs for all the tunnel groups.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn group-url** command. Each group can have multiple URLs or no URL.

Examples

The following example shows the **show webvpn group-url** command that displays the URLs for the tunnel group "frn-eng1" and the output of that command:

```
ciscoasa# show webvpn group-url
http://www.cisco.com
https://fra1.example.com
https://fra2.example.com
```

Related Commands

Command	Description
group-url	Specifies one or more URLs for the group.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn hostscan

To determine whether Hostscan is enabled, display the Hostscan version in the running configuration, determine which image is providing the Host Scan package, and to test a file to see if it is a valid Hostscan distribution package, use the show webvpn hostscan command in privileged EXEC mode.

show webvpn hostscan [**image** *filename*]

Syntax Description

filename	Specifies the name of a file to test for validity as a Hostscan distribution package. It must take the form **hostscan_4.1.04011-k9.pkg**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.5(2)	This command was added.
9.0(1)	Support for multiple context mode was added.

Examples

Use the **show webvpn hostscan** command to check the operational status of Hostscan. The CLI responds with a message indicating if Hostscan is installed and if it is enabled, if Host Scan is installed and if it is enabled, and which image is supplying the Host Scan package.

```
ciscoasa# show webvpn hostscan
```

These are the messages you could receive:

- Hostscan is not installed
- Hostscan n.n.n is currently installed and enabled

The message, “ Hostscan version n.n.n is currently installed ... ” means that the image is loaded on the ASA and in the running configuration. The image can be either enabled or not enabled. You can go to webvpn configuration mode and enter the **hostscan enable** command to enable CSD.

- Hostscan version n.n.n is currently installed but not enabled

Use the **show webvpn hostscan image** *filename* command to test a file to determine if a Hostscan distribution package is valid.

ciscoasa# **show webvpn hostscan image hostscan_4.1.04011-k9.pkg**

The CLI responds with one of the following messages when you enter this command:

- ERROR: This is not a valid Hostscan image file.

Make sure the filename is in the form the form **hostscan_n.n.n-k9.pkg**. If the Hostscan package does not have this naming convention, replace the file with one obtained from the Cisco download site for the version of Secure Client that you are using.

Then reenter the **show webvpn hostscan image** command. If the image is valid, use the **hostscan image** and **hostscan enable** commands in webvpn configuration mode to install and enable Hostscan.

- This is a valid Hostscan image:

Version : 4.1.4011

Built on : Mon July 27 15:46:44 MST 2015

Note that the CLI provides both the version and date stamp if the file is valid.

Related Commands

Command	Description
hostscan enable	Enables Hostscan for management and remote user access.
hostscan image	Copies the Hostscan image named in the command, from the flash drive specified in the path to the running configuration.

show webvpn hsts

To view information about HTTP Strict-Transport-Security (HSTS) on ASA, use the **show webvpn hsts** command from privileged EXEC mode.

show webvpn hsts host { **all** | **name** *hsts_hostname* }

Syntax Description

all	Displays information about all HSTS hosts.
name	Displays information about a specific HSTS host.
hsts_hostname	Specifies a particular HSTS host.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn hsts** command.

Example

The following example displays information about all the HSTS hosts:

```
ciscoasa#show webvpn hsts all
```

show webvpn kcd

Use the **show** webvpn kcd command in webvpn configuration mode to display the Domain Controller information and Domain join status on the ASA.

show webvpn kcd

Syntax Description

None.

Command Default

There are no defaults for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.4(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

The **show** webvpn kcd command in webvpn configuration mode displays the Domain Controller information and Domain join status on the ASA.

Examples

The following example shows important details to note from the **show webvpn kcd** command and the interpretation of the status message.

This example shows that the registration is under way and not finished:

ciscoasa # **show webvpn kcd**Kerberos Realm: CORP.TEST.INTERNALDomain Join: In-Progress

This example shows that a registration was successful and that the ASA has joined the domain:

```
ciscoasa# show webvpn kcd
Kerberos Realm: CORP.TEST.INTERNALDomain Join: Complete
```

Related Commands

Command	Description
clear aaa kerberos	Clears all the Kerberos tickets cached on the ASA.
kcd-server	Allows the ASA to join an Active Directory domain.

Command	Description
show aaa kerberos	Displays all the Kerberos tickets cached on the ASA.

show webvpn mus

To view information about Mobile User Security (MUS), use the **show webvpn mus** command in privileged EXEC mode.

show webvpn mus

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn mus** command.

Example

The following example displays information about Mobile User Security:

```
ciscoasa#show webvpn mus
No active WSA connections
```

show webvpn saml

To view information about the SAML identity provider, use the **show webvpn saml idp** command from privileged EXEC mode.

show webvpn saml idp

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn saml idp** command.

Example

The following example displays information about the SAML identity provider:

```
ciscoasa#show webvpn saml idp
```

show webvpn sso-server (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To display the operating statistics for Webvpn single sign-on servers, use the **show webvpn sso-server** command in privileged EXEC mode.

show webvpn sso-server [*name*]

Syntax Description

name	Optionally specifies the name of the SSO server. The server name must be between four and 31 characters in length.

Command Default

No default values or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Config-webvpn-sso-saml	• Yes	—	• Yes	—	—
Config-webvpn-sso-siteminder	• Yes	—	• Yes	—	—
Privileged EXEC	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated, due to support for SAML 2.0.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **show webvpn sso-server** command displays operating statistics for any and all SSO servers configured on the security device.

If no SSO server name argument is entered, statistics for all SSO servers display.

Examples

The following example, entered in privileged EXEC mode, displays statistics for a SiteMinder-type SSO server named example:

```
ciscoasa# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa#
The following example of the command issued without a specific SSO server name, displays
statistics for all configured SSO servers on the ASA:
ciscoasa#(config-webvpn)# show webvpn sso-server
Name: high-security-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: my-server
Type: SAML-v1.1-POST
Assertion Consumer URL:
Issuer:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
Name: server
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL:
Number of pending requests:        0
Number of auth requests:           0
Number of retransmissions:         0
Number of accepts:                 0
Number of rejects:                 0
Number of timeouts:                0
Number of unrecognized responses:  0
ciscoasa(config-webvpn)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder-type SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.

Command	Description
sso-server	Creates a single sign-on server.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

show webvpn statistics

To view the WebVPN event statistics, use the **show webvpn statistics** command from privileged EXEC mode.

show webvpn statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.14	The command was added.

Usage Guidelines

WebVPN must be running when you enter the **show webvpn statistics** command.

Example

The following example displays information about the WebVPN event statistics:

```
ciscoasa#show webvpn statistics
Total number of objects served         0
html                           0
js                             0
css                            0
vb                             0
java archive                   0
java class                     0
image                          0
undetermined                   0
Server compression statistics
Decompression success from server                 0
Unsolicited compression from server               0
Unsupported compression algorithm used by server   0
Decompression failure for server responses        0
IOBuf failure statistics
uib_create_with_channel                           0
uib_create_with_string                            0
uib_create_with_string_and_channel                0
uib_transfer                                      0
uib_add_filter                                    0
```

```
uib_yyread                                  0
uib_read                                    0
uib_set_buffer_max                          0
uib_set_eof_symbol                          0
        uib_get_capture_handle                      0
        uib_set_capture_handle                      0
        uib_buflen                                  0
        uib_bufptr                                  0
        uib_buf_endptr                              0
        uib_get_buf_offset                          0
        uib_get_buf_offset_addr                     0
        uib_get_nth_char                            0
        uib_consume                                 0
        uib_advance_bufptr                          0
```

show xlate

To display information about NAT sessions (xlates), use the **show xlate** command in privileged EXEC mode.

show xlate [**global** *ip1* [*-ip2*] [**netmask** *mask*]] [**local** *ip1* [*-ip2*] [**netmask** *mask*]] [**gport** *port1* [*-port2*]] [**lport** *port1* [*-port2*]] [**interface** *if_name*] [**type** *type*]

Syntax Description

count	Displays the translation count.
global *ip1*[-*ip2*]	(Optional) Displays the active translations by mapped IP address or range of addresses.
gport *port1*[-*port2*]	Displays the active translations by the mapped port or range of ports.
interface *if_name*	(Optional) Displays the active translations by interface.
local*ip1*[-*ip2*]	(Optional) Displays the active translations by real IP address or range of addresses.
lport *port1*[-*port2*]	Displays the active translations by real port or range of ports.
netmask *mask*	(Optional) Specifies the network mask to qualify the mapped or real IP addresses.
type *type*	(Optional) Displays the active translations by type. You can enter one or more of the following types: • **static** • **portmap** • **dynamic** • **twice-nat** When specifying more than one type, separate the types with a space.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was modified to support the new NAT implementation.
8.4(3)	The **e** flag was added to show use of extended PAT. In addition, the destination address to which the xlate is extended is shown.
9.0(1)	This command was modified to support IPv6.

Usage Guidelines

The **show xlate** command displays the contents of the translation slots.

When the **vpnclient** configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

In an ASA clustering environment, up to three xlates may be duplicated to different nodes in the cluster to handle a PAT session. One xlate is created on the unit that owns the connection. One xlate is created on a different unit to backup the PAT address. Finally, one xlate exists on the director that replicates the flow. In the case where the backup and director is the same unit, two instead of three xlates may be created.

If you create twice NAT rules without specifying a destination translation, the system interprets it as a static translation for any address. Thus, the NAT table includes a translation for 0.0.0.0/0 to 0.0.0.0/0. This rule is implied from your twice NAT rule.

Examples

The following is sample output from the **show xlate** command.

```
ciscoasa# show xlate
5 in use, 5 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
NAT from any:10.90.67.2 to any:10.9.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.90.67.2 to any:10.86.94.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.9.0.9, 10.9.0.10/31, 10.9.0.12/30,
    10.9.0.16/28, 10.9.0.32/29, 10.9.0.40/30,
    10.9.0.44/31 to any:0.0.0.0
    flags idle 277:05:26 timeout 0:00:00
NAT from any:10.1.1.0/24 to any:172.16.1.0/24
    flags idle 277:05:14 timeout 0:00:00
```

The following is sample output from the **show xlate** command showing use of the **e - extended** flag and the destination address to which the xlate is extended.

```
ciscoasa# show xlate
1 in use, 1 most used
Flags: D - DNS, i - dynamic, r - portmap, s - static, I - identity, T - twice
       e - extended
ICMP PAT from inside:10.2.1.100/6000 to outside:172.16.2.200/6000(172.16.2.99)
 flags idle 0:00:06 timeout 0:00:30
TCP PAT from inside:10.2.1.99/5 to outside:172.16.2.200/5(172.16.2.90)
 flags idle 0:00:03 timeout 0:00:30
UDP PAT from inside:10.2.1.101/1025 to outside:172.16.2.200/1025(172.16.2.100)
 flags idle 0:00:10 timeout 0:00:30
```

The following is sample output from the **show xlate** command showing a translation from IPv4 to IPv6.

```
ciscoasa# show xlate
1 in use, 2 most used
NAT from outside:0.0.0.0/0 to in:2001::/96
flags sT idle 0:16:16 timeout 0:00:00
```

Related Commands

Command	Description
clear xlate	Clears current translation and connection information.
show conn	Displays all active connections.
show local-host	Displays the local host network information.
show uauth	Displays the currently authenticated users.

show zone

To shows zone ID, context, security level, and members, use the **show zone** command in privileged EXEC mode.

show zone [*name*]

Syntax Description

name	(Optional) Identifies the zone name set by the **zone** command.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Usage Guidelines

To view the zone configuration, use the **show running-config zone** command.

Examples

See the following output for the **show zone** command:

```
ciscoasa# show zone outside-zone
Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

Related Commands

Command	Description
clear configure zone	Clears the zone configuration.
clear conn zone	Clears zone connections.
clear local-host zone	Clears zone hosts.
show asp table routing	Shows the accelerated security path tables for debugging purposes, and shows the zone associated with each route.

Command	Description
show asp table zone	Shows the accelerated security path tables for debugging purposes.
show conn long	Shows connections information for zones.
show local-host zone	Shows the network states of local hosts within a zone.
show nameif zone	Shows the interface names and zone names.
show route zone	Shows the routes for zone interfaces.
show running-config zone	Shows the zone configuration.
show zone	Shows zone ID, context, security level, and members.
zone	Configures a traffic zone.
zone-member	Assigns an interface to a traffic zone.

shox – sn

shun

To block connections from an attacking host, use the shun command in privileged EXEC mode. To disable a shun, use the **no** form of this command.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]
no shun *source_ip* [**vlan** *vlan_id*]

Syntax Description

dest_port	(Optional) Specifies the destination port of a current connection that you want to drop when you place the shun on the source IP address.
dest_ip	(Optional) Specifies the destination address of a current connection that you want to drop when you place the shun on the source IP address.
protocol	(Optional) Specifies the IP protocol of a current connection that you want to drop when you place the shun on the source IP address, such as UDP or TCP. By default, the protocol is 0 (any protocol).
source_ip	Specifies the address of the attacking host. If you only specify the source IP address, all future connections from this address are dropped; current connections remain in place. To drop a current connection and also place the shun, specify the additional parameters of the connection. Note that the shun remains in place for all future connections from the source IP address, regardless of destination parameters.
source_port	(Optional) Specifies the source port of a current connection that you want to drop when you place the shun on the source IP address.
vlan_id	(Optional) Specifies the VLAN ID where the source host resides.

Command Default

The default protocol is 0 (any protocol).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The shun command lets you block connections from an attacking host. All future connections from the source IP address are dropped and logged until the blocking function is removed manually or by the Cisco IPS sensor.

The blocking function of the shun command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the ASA configuration.

Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed. If you add a new interface or replace the same interface (using the same name), then you must add that interface to the IPS sensor if you want the IPS sensor to monitor that interface.

Examples

The following example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the ASA connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

Apply the shun command using the following options:

```
ciscoasa# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The command deletes the specific current connection from the ASA connection table and also prevents all future packets from 10.1.1.27 from going through the ASA.

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
show conn	Shows all active connections.
show shun	Displays the shun information.

shutdown (ca-server)

To disable the local Certificate Authority (CA) server and render the enrollment interface inaccessible to users, use the **shutdown** command in CA server configuration mode. To enable the CA server, lock down the configuration from changes, and to render the enrollment interface accessible, use the **no** form of this command.

[**no**] **shutdown**

Syntax Description

This command has no arguments or keywords.

Command Default

Initially, by default, the CA server is shut down.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

This command in CA server mode is similar to the **shutdown** command in interface mode. At setup time, the local CA server is shutdown by default and must be enabled using the **no shutdown** command. When you use the **no shutdown** command for the first time, you enable the CA server and generate the CA server certificate and keypair.

Note The CA configuration cannot be changed once you lock it and generate the CA certificate by issuing the **no shutdown** command.

To enable the CA server and lock down the current configuration with the **no shutdown** command, a 7-character password is required to encode and archive a PKCS12 file containing the CA certificate and keypair that is to be generated. The file is stored to the storage identified by a previously specified **database path** command.

Examples

The following example disables the local CA server and renders the enrollment interface inaccessible:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# shutdown
```

```
ciscoasa
(config-ca-server)
#
```

The following example enables the local CA server and makes the enrollment interface accessible:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no shutdown
ciscoasa
(config-ca-server)
#
ciscoasa
(config-ca-server)
# no shutdown
% Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: caserver
Re-enter password: caserver
Keypair generation process begin. Please wait...
ciscoasa
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to the CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
show crypto ca server	Displays the status of the CA configuration.

shutdown (interface)

To disable an interface, use the **shutdown** command in interface configuration mode. To enable an interface, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

All physical interfaces are shut down by default. Allocated interfaces in security contexts are not shut down in the configuration.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

The default state of an interface depends on the type and the context mode.

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Note This command only disables the software interface. The physical link remains up, and the directly connected device is still recognized as being up even when the corresponding interface is configured with the **shutdown** command.

Examples

The following example enables a main interface:

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

The following example enables a subinterface:

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

The following example shuts down the subinterface:

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.

sip address

To provide the Session Initiation Protocol (SIP) server IP address to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **sip address** command in ipv6 dhcp pool configuration mode. To remove the SIP server, use the **no** form of this command.

sip address *sip_ipv6_address*
no sip address *sip_ipv6_address*

Syntax Description

sip_ipv6_address	Specifies the SIP server IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the SIP server, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
sip domain-name eng.example.com
sip server 2001:DB8:2::8
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
```

```
sip domain-name it.example.com
sip server 2001:DB8:2::8
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.

Command	Description
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

sip domain-name

To provide the Session Initiation Protocol (SIP) domain name to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **sip domain-name** command in ipv6 dhcp pool configuration mode. To remove the SIP domain name, use the **no** form of this command.

sip domain-name *sip_domain_name*
no sip domain-name *sip_domain_name*

Syntax Description

sip_domain_name	Specifies the SIP domain name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the SIP domain name, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
sip domain-name eng.example.com
sip server 2001:DB8:2::8
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
```

```
sip domain-name it.example.com
sip server 2001:DB8:2::8
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.

Command	Description
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

site-id

For inter-site clustering, use the **site-id** command in cluster group configuration mode. To remove the site ID, use the **no** form of this command.

site-id*number*
no site-id *number*

Syntax Description

number	Sets the site ID, between 1 and 8.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.5(1)	This command was added.
9.5(2)	You can now enter this command in transparent mode for use with LISP flow mobility.
9.7(1)	For FXOS, you must set the site ID in the FXOS logical device settings; you cannot change it on the ASA.

Usage Guidelines

You can configure each cluster chassis to belong to a separate site ID.

Site IDs work with site-specific MAC addresses. Packets sourced from the ASA cluster use a site-specific MAC address, while packets received by the cluster use a global MAC address. This feature prevents the switches from learning the same global MAC address from both sites on two different ports, which causes MAC flapping; instead, they only learn the site MAC address. Site-specific MAC addresses are supported for routed mode using Spanned EtherChannels only.

Site IDs are also used to enable flow mobility using LISP inspection.

Configure the MAC addresses on the master unit using the **mac-address site-id** command, and then assign each unit (master and slave) to a site using the **site-id** command as part of the cluster bootstrap configuration.

Examples

The following example configures site-specific MAC addresses for port-channel 2, and assigns the master unit to site 1:

```
ciscoasa(config)# interface port-channel 2
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4
ciscoasa(config)# cluster group pod1
ciscoasa(cfg-cluster)# local-unit unit1
ciscoasa(cfg-cluster)# cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
ciscoasa(cfg-cluster)# site-id 1
ciscoasa(cfg-cluster)# priority 1
ciscoasa(cfg-cluster)# key chuntheunavoidable
ciscoasa(cfg-cluster)# enable noconfirm
```

Related Commands

Command	Description
clacp system-mac	When using spanned EtherChannels, the ASA uses cLACP to negotiate the EtherChannel with the neighbor switch.
cluster group	Names the cluster and enters cluster configuration mode.
cluster-interface	Specifies the cluster control link interface.
cluster interface-mode	Sets the cluster interface mode.
conn-rebalance	Enables connection rebalancing.
console-replicate	Enables console replication from slave units to the master unit.
enable (cluster group)	Enables clustering.
health-check	Enables the cluster health check feature, which includes unit health monitoring and interface health monitoring.
key	Sets an authentication key for control traffic on the cluster control link.
local-unit	Names the cluster member.
mac-address site-id	Configures a site-specific MAC address for each site.
mtu cluster-interface	Specifies the maximum transmission unit for the cluster control link interface.
priority (cluster group)	Sets the priority of this unit for master unit elections.

site-periodic-garp interval

To customize the gratuitous ARP (GARP) interval for clustering, use the **site-periodic-garp interval** command in cluster group configuration mode. To disable GARP, use the **no** form of this command.

site-periodic-garp interval *seconds*
no site-periodic-garp interval

Syntax Description

seconds	Sets the time in seconds between GARP generation, between 1 and 1000000 seconds. The default is 290 seconds.

Command Default

The default interval is 290 seconds.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.12(1)	Command added.

Usage Guidelines

The ASA generates gratuitous ARP (GARP) packets to keep the switching infrastructure up to date: the highest priority member at each site periodically generates GARP traffic for the global MAC/IP addresses.

When using per-site MAC and IP addresses, packets sourced from the cluster use a site-specific MAC address and IP address, while packets received by the cluster use a global MAC address and IP address. If traffic is not generated from the global MAC address periodically, you could experience a MAC address timeout on your switches for the global MAC address. After a timeout, traffic destined for the global MAC address will be flooded across the entire switching infrastructure, which can cause performance and security concerns.

GARP is enabled by default when you set the site ID for each unit and the site MAC address for each Spanned EtherChannel.

Examples

The following example sets the GARP interval to 500 seconds:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

Related Commands

Command	Description
cluster group	Enters cluster group mode.

site-redundancy

To protect cluster flows from a site failure, use the **site-redundancy** command in cluster group configuration mode. To disable site redundancy, use the **no** form of this command.

site-redundancy
no site-redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Site redundancy is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Cluster group configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.9(1)	Command added.

Usage Guidelines

To protect flows from a site failure, you can enable site redundancy. If the connection backup owner is at the same site as the owner, then an additional backup owner will be chosen from another site to protect flows from a site failure.

Director localization and site redundancy are separate features; you can configure one or the other, or configure both.

Examples

The following example sets the interval to 300 ms:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# site-redundancy
```

Related Commands

Command	Description
director-localization	Enables director localization, which improves performance and reduces round-trip time latency for inter-site clustering for data centers.

sla monitor

To create an SLA operation, use the **sla monitor** command in global configuration mode. To remove the SLA operation, use the **no** form of this command.

sla monitor *sla_id*
no sla monitor *sla_id*

Syntax Description

sla_id	Specifies the ID of the SLA being configured. If the SLA does not already exist, it is created. Valid values are from 1 to 2147483647.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

The **sla monitor** command creates SLA operations and enters SLA Monitor configuration mode. Once you enter this command, the command prompt changes to ciscoasa (config-sla-monitor)# to indicate that you are in SLA Monitor configuration mode. If the SLA operation already exists, and a type has already been defined for it, then the prompt appears as ciscoasa (config-sla-monitor-echo)#. You can create a maximum of 2000 SLA operations. Only 32 SLA operations may be debugged at any time.

The **no sla monitor** command removes the specified SLA operation and the commands used to configure that operation.

After you configure an SLA operation, you must schedule the operation with the **sla monitor schedule** command. You cannot modify the configuration of the SLA operation after scheduling it. To modify the the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

To display the current configuration settings of the operation, use the **show sla monitor configuration** command. To display operational statistics of the SLA operation, use the **show sla monitor operation-state command**. To see the SLA commands in the configuration, use the **show running-config sla monitor** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
frequency	Specifies the rate at which the SLA operation repeats.
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor schedule	Schedules the SLA operation.
timeout	Sets the amount of time the SLA operation waits for a response.
track rtr	Creates a tracking entry to poll the SLA.

sla monitor schedule

To schedule an SLA operation, use the **sla monitor schedule** command in global configuration mode. To remove SLA operation schedule, and place the operation in the pending state, use the **no** form of this command.

sla monitor schedule *sla-id* [**life** { **forever** | *seconds* }] [**start-time** { *hh:mm* [*:ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh:mm:ss* }] [**ageout** *seconds*] [**recurring**]
no sla monitor schedule *sla-id*

Syntax Description

after *hh* : *mm* : *ss*	Indicates that the operation should start the specified number of hours, minutes, and seconds after the command was entered.
ageout *seconds*	(Optional) Specifies the number of seconds to keep the operation in memory when it is not actively collecting information. After an SLA operation ages out, it is removed from the running configuration.
day	Number of the day to start the operation on. Valid values are from 1 to 31. If a day is not specified, then the current day is used. If you specify a day you must also specify a month.
hh : *mm* [: *ss*]	Specifies an absolute start time in 24-hour notation. Seconds are optional. The next time the specified time occurs is implied unless you specify a *month* and a *day* .
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Sets the number of seconds the operation actively collects information.
month	(Optional) Name of the month to start the operation in. If a month is not specified, then the current month is used. I f you specify a month you must also specify a day. You can enter the full English name of the month or just the first three letters.
now	Indicates that the operation should start as soon as the command is entered.
pending	Indicates that no information is collected. This is the default state.
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.
sla-id	The ID of the SLA operation being scheduled.
start-time	Sets the time when the SLA operation starts.

Command Default

The defaults are as follows:

- SLA operations are in the **pending** state until the scheduled time is met. This means that the operation is enabled but not actively collecting data.
- The default **ageout** time is 0 seconds (never ages out).
- The default **life** is 3600 seconds (one hour).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

When an SLA operation is in an active state, it immediately begins collecting information. The following time line shows the age-out process of the operation:

```
W---------------------X---------------------Y---------------------Z
```

- W is the time the SLA operation was configured with the **sla monitor** command.
- X is the start time of the SLA operation. This is when the operation became “active”.
- Y is the end of life as configured with the **sla monitor schedule** command (the **life** seconds have counted down to zero).
- Z is the age out of the operation.

The age out process, if used, starts counting down at W, is suspended between X and Y, and is reset to its configured size are starts counting down again at Y. When an SLA operation ages out, the SLA operation configuration is removed from the running configuration. It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation configuration time and start time (X and W) must be less than the age-out seconds.

The **recurring** keyword is only supported for scheduling single SLA operations. You cannot schedule multiple SLA operations using a single **sla monitor schedule** command. The **life** value for a recurring SLA operation should be less than one day. The **ageout** value for a recurring operation must be “never” (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the recurring option is not specified, the operations are started in the existing normal scheduling mode.

You cannot modify the configuration of the SLA operation after scheduling it. To modify the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

Examples

The following example shows SLA operation 25 scheduled to begin actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity. When this SLA operation ages out, all configuration information for the SLA operation is removed from the running configuration.

```
ciscoasa(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

The following example shows SLA operation 1 schedule to begin collecting data after a 5-minute delay. The default life of one hour applies.

```
ciscoasa(config)# sla monitor schedule 1 start after 00:05:00
```

The following example shows SLA operation 3 scheduled to begin collecting data immediately and is scheduled to run indefinitely:

```
ciscoasa(config)# sla monitor schedule 3 life forever start-time now
```

The following example shows SLA operation 15 scheduled to begin automatically collecting data every day at 1:30 a.m.:

```
ciscoasa(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor	Defines an SLA monitoring operation.

smart-tunnel auto-signon enable(Deprecated)

To enable smart tunnel auto sign-on in clientless (browser-based) SSL VPN sessions, use the **smart-tunnel auto-signon enable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

To remove the **smart-tunnel auto-signon enable** command from the group policy or username and inherit it from the default group-policy, use the **no** form of this command.

no smart-tunnel auto-signon enable *list* [**domain** *domain*] [**port** *port*] [**realm** *realm string*]

Syntax Description

domain *domain*	(Optional). Name of the domain to be added to the username during authentication. If you enter a domain, enter the **use-domain** keyword in the list entries.
list	The name of a smart tunnel auto sign-on list already present in the ASA webvpn configuration. To view the smart tunnel auto sign-on list entries in the SSL VPN configuration, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.
port	Specifies which port performs auto sign-on.
realm	Configures a realm for the authentication.

Command Default

No defaults exist for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
8.4(1)	Optional *realm* and *port* arguments were added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.

You must use the **smart-tunnel auto-signon** *list* command to create a list of servers first. You can assign only one list to a group policy or username.

A realm string is associated with the protected area of the website and is passed back to the browser either in the authentication prompt or in the HTTP headers during authentication. If adminstrators do not know the corresponding realm, they should perform logon once and get the string from the prompt dialog.

Administrators can now optionally specify a port number for the corresponding hosts. For Firefox, if no port number is specified, auto sign-on is performed on HTTP and HTTPS, accessed by the default port numbers 80 and 443 respectively.

Examples

The following commands enable the smart tunnel auto sign-on list named HR:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR
ciscoasa(config-group-webvpn)
```

The following command enables the smart tunnel auto sign-on list named HR and adds the domain named CISCO to the username during authentication:

```
ciscoasa(config-group-webvpn)# smart-tunnel auto-signon enable HR domain CISCO
```

The following command removes the smart tunnel auto sign-on list named HR from the group policy and inherits the smart tunnel auto sign-on list command from the default group policy:

```
ciscoasa(config-group-webvpn)# no smart-tunnel auto-signon enable HR
```

Related Commands

Command	Description
smart-tunnel auto-signon *list*	Creates a list of servers for which to automate the submission of credentials in smart tunnel connections.
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration on the ASA.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel *list*	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel auto-signon list(Deprecated)

To create a list of servers for which to automate the submission of credentials in smart tunnel connections, use the **smart-tunnel auto-signon list** command in webvpn configuration mode.Use this command for each server you want to add to a list.

To remove an entry from a list, use the **no** form of this command, specifying both the list and the IP address or hostname, as it appears in the ASA configuration.

no smart-tunnel auto-signon *list* [**use-domain**] { **ip** *ip-address* [*netmask*] **| host** *hostname-mask* }

To display the smart tunnel auto sign-on list entries, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.

To remove an entire list of servers from the ASA configuration, use the **no** form of the command, specifying only the list.

no smart-tunnel auto-signon *list*

Syntax Description

host	Server to be identified by its host name or wildcard mask.
hostname-mask	Host name or wildcard mask to auto-authenticate to.
ip	Server to be identified by its IP address and netmask.
ip-address [*netmask*]	Sub-network of hosts to auto-authenticate to.
list	Name of a list of remote servers. Use quotation marks around the name if it includes a space. The string can be up to 64 characters. The ASA creates the list if it is not present in the configuration. Otherwise, it adds the entry to the list.
use-domain	(Optional) Add the Windows domain to the username if authentication requires it. If you enter this keyword, be sure to specify the domain name when assigning the smart tunnel list to one or more group policies, or usernames.

Command Default

No defaults exist for this command.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(4)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The smart-tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.

Following the population of a smart tunnel auto sign-on list, use the **smart-tunnel auto-signon enable** *list* command in group policy webvpn or username webvpn mode to assign the list.

Examples

The following command adds all hosts in the subnet and adds the Windows domain to the username if authentication requires it:

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon HR use-domain ip 192.32.22.56 255.255.255.0
```

The following command removes that entry from the list:

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR use-domain ip 192.32.22.56
255.255.255.0
```

The command shown above also removes the list named HR if the entry removed is the only entry in the list. Otherwise, the following command removes the entire list from the ASA configuration:

```
ciscoasa(config-webvpn)# no smart-tunnel auto-signon HR
```

The following command adds all hosts in the domain to the smart tunnel auto sign-on list named intranet:

```
ciscoasa(config-webvpn)# smart-tunnel auto-signon intranet host *.exampledomain.com
```

The following command removes that entry from the list:

```
ciscoasa(config-webvpn)# no smart-tunnel
 auto-signon intranet host *.exampledomain.com
```

Related Commands

Command	Description
smart-tunnel auto-signon enable	Enables smart tunnel auto sign-on for the group policy or username specified in the command mode.
smart-tunnel auto-signon enable *list*	Assigns a smart tunnel auto sign-on list to a group policy or username
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.

Command	Description
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.

smart-tunnel auto-start(Deprecated)

To start smart tunnel access automatically upon user login in a clientless (browser-based) SSL VPN session, use the **smart-tunnel auto-start** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel auto-start *list*

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

list	*list* is the name of a smart tunnel list already present in the ASA webvpn configuration. To view any smart tunnel list entries already present in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—
Username webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

This command requires that you use the **smart-tunnel list** command to create the list of applications first.

This option to start smart tunnel access upon user login applies only to Windows.

Examples

The following commands start smart tunnel access for a list of applications named apps1:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel auto-start apps1
ciscoasa(config-group-webvpn)
```

The following commands remove the list named apps1 from the group policy and inherit the smart tunnel commands from the default group policy:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the Clientless SSL VPN configuration, including all smart tunnel list entries.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel disable(Deprecated)

To prevent smart tunnel access through clientless (browser-based) SSL VPN sessions, use the **smart-tunnel disable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel disable

To remove a **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—
Username webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

By default, smart tunnels are not enabled, so the **smart-tunnel disable** command is necessary only if the (default) group policy or username configuration contains a **smart-tunnel auto-start** or **smart-tunnel enable** command that you do not want applied for the group policy or username in question.

Examples

The following commands prevent smart tunnel access:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel disable
ciscoasa(config-group-webvpn)
```

Related Commands

Command	Description
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel enable(Deprecated)

To enable smart tunnel access through clientless (browser-based) SSL VPN sessions, use the **smart-tunnel enable** command in group-policy webvpn configuration mode or username webvpn configuration mode.

smart-tunnel enable *list*

To remove the **smart-tunnel** command from the group policy or username and inherit the [**no**] **smart-tunnel** command from the default group-policy, use the **no** form of the command.

no smart-tunnel

Syntax Description

list	*list* is the name of a smart tunnel list already present in the ASA webvpn configuration. To view the smart tunnel list entries in the SSL VPN configuration, enter the **show running-config webvpn** command in privileged EXEC mode.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—
Username webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

The **smart-tunnel enable** command assigns a list of applications eligible for smart tunnel access to a group policy or username. It requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the clientless-SSL-VPN portal page. Alternatively, you can use the **smart-tunnel auto-start** command to start smart tunnel access automatically upon user login.

Both commands require that you use the **smart-tunnel list** command to create the list of applications first.

Examples

The following commands enable the smart tunnel list named apps1:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# smart-tunnel enable apps1
ciscoasa(config-group-webvpn)
```

The following commands remove the list named apps1 from the group policy and inherit the smart tunnel list from the default group policy:

```
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# no smart-tunnel
ciscoasa(config-group-webvpn)
```

Related Commands

Command	Description
show running-config webvpn	Displays the Clientless SSL VPN configuration, including all smart tunnel list entries.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel list	Adds an entry to a list of applications that can use a Clientless SSL VPN session to connect to private sites.

smart-tunnel list(Deprecated)

To populate a list of applications that can use a clientless (browser-based) SSL VPN session to connect to private sites, use the **smart-tunnel list** command in webvpn configuration mode. To remove an application from a list, use the **no** form of the command, specifying the entry. To remove an entire list of applications from the ASA configuration, use the **no** form of the command, specifying only the list.

[**no**] **smart-tunnel list** *list application path* [**platform** *OS*] [*hash*]
no smart-tunnel list *list*

Syntax Description

application	Name of the application to be granted smart tunnel access. The string can be up to 64 characters.
hash	(Optional and applicable only for Windows) To obtain this value, enter the checksum of the application (that is, the checksum of the executable file) into a utility that calculates a hash using the SHA-1 algorithm. One example of such a utility is the Microsoft File Checksum Integrity Verifier (FCIV), which is available at http://support.microsoft.com/kb/841290/ . After installing FCIV, place a temporary copy of the application to be hashed on a path that contains no spaces (for example, c:/fciv.exe), then enter **fciv.exe -sha1** *application* at the command line (for example, **fciv.exe -sha1 c:\msimn.exe**) to display the SHA-1 hash. The SHA-1 hash is always 40 hexadecimal characters.
list	Name of a list of applications or programs. Use quotation marks around the name if it includes a space. The CLI creates the list if it is not present in the configuration. Otherwise, it adds the entry to the list.
path	For Mac OS, the full path to the application. For Windows, the filename of the application; or a full or partial path to the application, including its filename. The string can be up to 128 characters.
platform *OS*	(Optional if the OS is Microsoft Windows) Enter **windows or mac** to specify the host of the application.

Command Default

Windows is the default platform.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	**platform** *OS* was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

You can configure more than one smart tunnel list on an ASA, but you cannot assign more than one smart tunnel list to a given group policy or username. To populate a smart tunnel list, enter the **smart-tunnel list** command once for each application, entering the same *list* string, but specifying an *application* and *path* that is unique for the OS. Enter the command once for each *OS* you want the list to support.

The session ignores a list entry if the OS does not match the one indicated in the entry. It also ignores an entry if the path to the application is not present.

To view the smart tunnel list entries in the SSL VPN configuration, enter the **show running-config webvpn smart-tunnel** command in privileged EXEC mode.

The *path* must match the one on the computer, but it does not have to be complete. For example, the *path* can consist of nothing more than the executable file and its extension.

Smart tunnels have the following requirements:

- The remote host originating the smart tunnel connection must be running a 32-bit version of Microsoft Windows Vista, Windows XP, or Windows 2000; or Mac OS 10.4 or 10.5.
- Users of Microsoft Windows Vista who use smart tunnels or port forwarding must add the URL of the ASA to the Trusted Site zone. To access the Trusted Site zone, they must start Internet Explorer and choose the Tools > Internet Options > Security tab. Vista users can also disable Protected Mode to facilitate smart tunnel access; however, we recommend against this method because it increases the computer’s vulnerability to attack.
- The browser must be enabled with Java, Microsoft ActiveX, or both.
- Smart tunnel support for Mac OS requires Safari 3.1.1 or later.

On Microsoft Windows, only Winsock 2, TCP-based applications are eligible for smart tunnel access.

On Mac OS, applications using TCP that are dynamically linked to the SSL library can work over a smart tunnel. The following types of applications do not work over a smart tunnel:

- Applications using dlopen or dlsym to locate libsocket calls
- Statically linked applications to locate libsocket calls
- Mac OS applications that use two-level name spaces.
- Mac OS, console-based applications, such as Telnet, SSH, and cURL.
- Mac OS, PowerPC-type applications. To determine the type of a Mac OS application, right-click its icon and select Get Info.

On Mac OS, only applications started from the portal page can establish smart tunnel sessions. This requirement includes smart tunnel support for Firefox. Using Firefox to start another instance of Firefox during the first use of a smart tunnel requires the user profile named csco_st. If this user profile is not present, the session prompts the user to create one.

The following limitations apply to smart tunnels:

- If the remote computer requires a proxy server to reach the ASA, the URL of the terminating end of the connection must be in the list of URLs excluded from proxy services. In this configuration, smart tunnels support only basic authentication.
- The smart tunnel auto sign-on feature supports only applications communicating HTTP and HTTPS using the Microsoft WININET library on a Microsoft Windows OS. For example, Microsoft Internet Explorer uses the WININET dynamic linked library to communicate with web servers.
- A group policy or local user policy supports no more than one list of applications eligible for smart tunnel access and one list of smart tunnel auto sign-on servers.
- A stateful failover does not retain smart tunnel connections. Users must reconnect following a failover.

Note A sudden problem with smart tunnel access may be an indication that a *path* value is not up-to-date with an application upgrade. For example, the default path to an application typically changes following the acquisition of the company that produces the application and the next upgrade.

Entering a hash provides a reasonable assurance that clientless SSL VPN does not qualify an illegitimate file that matches the string you specified in the *path*. Because the checksum varies with each version or patch of an application, the *hash* you enter can only match one version or patch on the remote host. To specify a *hash* for more than one version of an application, enter the **smart-tunnel list** command once for each version, entering the same *list* string, but specifying the unique *application* string and unique *hash* value in each command.

Note You must maintain the smart tunnel list in the future if you enter *hash* values and you want to support future versions or patches of an application with smart tunnel access. A sudden problem with smart tunnel access may be an indication that the application list containing *hash* values is not up-to-date with an application upgrade. You can avoid this problem by not entering a *hash*.

Following the configuration of a smart tunnel list, use the **smart-tunnel auto-start** or **smart-tunnel enable** command to assign the list to group policies or usernames.

Examples

The following command adds the Microsoft Windows application Connect to a smart tunnel list named apps1:

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 LotusSametime connect.exe
```

The following command adds the Windows application msimn.exe and requires that the hash of the application on the remote host match the last string entered to qualify for smart tunnel access:

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 OutlookExpress msimn.exe
4739647b255d3ea865554e27c3f96b9476e75061
```

The following command provides smart tunnel support for the Mac OS browser Safari:

```
ciscoasa(config-webvpn)# smart-tunnel list apps1 Safari /Applications/Safari platform mac
```

Related Commands

Command	Description
show running-config webvpn smart-tunnel	Displays the smart tunnel configuration on the ASA.
smart-tunnel auto-start	Starts smart tunnel access automatically upon user login.
smart-tunnel disable	Prevents smart tunnel access.
smart-tunnel enable	Enables smart tunnel access upon user login, but requires the user to start smart tunnel access manually, using the **Application Access** > **Start Smart Tunnels** button on the Clientless SSL VPN portal page.

smart-tunnel network(Deprecated)

To create a list of hosts to use for configuring smart tunnel policies, use the **smart-tunnel network** command in webvpn configuration mode. To disallow a list of hosts for smart tunnel policies, use the **no** form of this command.

smart-tunnel network
no smart-tunnel network

Syntax Description

host *host mask*	The hostname mask, such as *.cisco.com.
ip *ip address*	The IP address of a network.
netmask	The Netmask of a network.
network name	The name of the network to apply to tunnel policy.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.3(1)	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

When the smart tunnel is turned on, you can allow traffic outside of the tunnel with the **smart-tunnel network** command, which configures the network (a set of hosts), and the **smart-tunnel tunnel-policy** command, which uses the specified smart-tunnel network to enforce a policy on a user.

Examples

The following is a sample of how the **smart-tunnel network** command is used:

```
ciscoasa(config-webvpn)# smart-tunnel network testnet ip 192.168.0.0 255.255.255
```

Related Commands

Command	Description
smart-tunnel tunnel-policy	Uses the specified smart-tunnel network to enforce a policy on a user.

smart-tunnel tunnel-policy(Deprecated)

To apply smart tunnel tunnel policies to a particular group or user policy, use the **smart-tunnel tunnel-policy** command in configuration webvpn mode. To unapply smart tunnel tunnel policies to a particular group, use the [no] form of this command.

smart-tunnel tunnel-policy
no smart-tunnel tunnel-policy

Syntax Description

excludespecified	Tunnels only networks that are outside of the networks specified by network name.
network name	Lists networks to be tunneled.
tunnelall	Makes everything tunneled (encrypted).
tunnelspecified	Tunnels only networks specified by network name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.3.1	This command was added.
9.17(1)	This command was deprecated due to support removal for web VPN.

Usage Guidelines

When the smart tunnel is turned on, you can allow traffic outside of the tunnel with the **smart-tunnel network** command, which configures the network (a set of hosts), and the **smart-tunnel tunnel-policy** command, which uses the specified smart-tunnel network to enforce a policy on a user.

Examples

The following is a sample of how the **smart-tunnel tunnel-policy** command is used:

```
ciscoasa(config-username-webvpn)# smart-tunnel tunnel-policy tunnelspecified testnet
```

Related Commands

Command	Description
smart-tunnel network	Creates a list of hosts for configuring smart tunnel policies.

smtp from-address

To specify the e-mail address to use in the E-mail From: field for all e-mails generated by the local CA server (such as distribution of one-time passwords) use the **smtp from-address** command in CA server configuration mode. To reset the e-mail address to the default, use the **no** form of this command.

smtp from-address *e-mail_address*
no smtp from-address

Syntax Description

e-mail_address	Specifies the e-mail address appearing in the From: field of all e-mails generated by the CA server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example specifies that the From: field of all e-mails from the local CA server include ca-admin@asa1-ca.example.com:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# smtp from-address ca-admin@asa1-ca.example.com
ciscoasa
(config-ca-server)
#
```

The following example resets the From: field of all e-mails from the local CA server to the default address admin@asa1-ca.example.com:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# smtp from-address admin@asa1-ca.example.com
ciscoasa
```

```
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
smtp subject	Customizes the text to appear in the subject field of all e-mails generated by the local CA server.

smtp subject

To customize the text that appears in the subject field of all e-mails generated by the local Certificate Authority (CA) server (such as distribution of one-time passwords), use the **smtp subject** command in CA server configuration mode. To reset the text to the default, use the **no** form of this command.

smtp subject *subject-line*
no smtp subject

Syntax Description

subject-line	Specifies the text appearing in the Subj: field of all e-mails sent from the CA server. The maximum number of characters is 127.

Command Default

By default, the text in the Subj: field is "Certificate Enrollment Invitation".

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ca server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Examples

The following example specifies that the text *Action: Enroll for a certificate* appear in the Subj: field of all e-mails from the CA server:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# smtp subject Action: Enroll for a certificate
ciscoasa
(config-ca-server)
#
```

The following example resets the Subj: field text for all e-mails from the CA server to the default text "Certificate Enrollment Invitation":

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no smtp subject
ciscoasa
```

```
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the local CA server.

smtps (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To enter SMTPS configuration mode, use the **smtps** command in global configuration mode. To remove any commands entered in SMTPS command mode, use the **no** version of this command. SMTPS is a TCP/IP protocol that lets you to send e-mail over an SSL connection.

smtps
no smtps

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.

Examples

The following example shows how to enter SMTPS configuration mode:

```
ciscoasa
(config)#
 smtps
ciscoasa(config-smtps)#
```

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
show running-config smtps	Displays the running configuration for SMTPS.

smtp-server

To configure an SMTP server, use the **smtp-server** command in global configuration mode. To remove the attribute from the configuration, use the **no** form of this command.

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*] *backup-smpt-server-ip-address*]
no smtp-server

Syntax Description

primary-smpt-server-ip-address	Identifies the primary SMTP server. Use either an IP address or hostname (configured using the **name** command).
backup-smpt-server-ip-address	(Optional) Identifies a backup SMTP server to relay event messages if the primary SMTP server is unavailable. Use either an IP address or hostname (configured using the **name** command).
primary_interface	(Optional) Identifies the primary interface name that can be used for reaching the primary smtp servers.
backup_interface	(Optional) Identifies a backup interface name that can be used for reaching the smtp backup server.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.5(2)	This command was deprecated.
9.13(1)	Primary and backup interface names can be optionally provided to connect with the appropriate smtp servers for logging.

Usage Guidelines

The ASA includes an internal SMTP client that the Events system can use to notify external entities that a certain event has occurred. You can configure SMTP servers to receive these event notices, and then forward them to specified e-mail addresses. The SMTP facility is active only when you enable E-mail events to the ASA. This command also allows interface association to identify the routing table to be used for logging—management routing table or data routing table. If no interface is provided, ASA would refer to management routing table lookup, and if no proper route entry is present, it would look at the data routing table.

Examples

The following examples show how to set an SMTP server with an IP address of 10.1.1.24, and a backup SMTP server with an IP address of 10.1.1.34:

```
ciscoasa
(config)#
 smtp-server 10.1.1.24 10.1.1.34
ciscoasa
(config)#
 smtp-server 10.1.1.24
ciscoasa
(config)#
 smtp-server management 10.1.1.24 outside 10.1.1.34
ciscoasa
(config)#
 smtp-server management 10.1.1.24
```

snmp cpu threshold rising

To configure the threshold value for a high CPU threshold and the threshold monitoring period, use the **snmp cpu threshold rising** command in global configuration mode. To not configure the threshold value and threshold monitoring period, use the **no** form of this command.

snmp cpu threshold rising *threshold_value monitoring_period*
no snmp cpu threshold rising *threshold_value monitoring_period*

Syntax Description

monitoring_period	Defines the monitoring period in minutes.
threshold_value	Defines the threshold level as a percentage of CPU usage.

Command Default

If the **snmp cpu threshold rising** command is not configured, the default for the high threshold level is set at over 70 percent of CPU usage, and the default for the critical threshold level isset at over 95 percent of CPU usage. The default monitoring period is set to one minute.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added. Does not apply to the ASA Services Module.

Usage Guidelines

You cannot configure the critical CPU threshold level, which is maintained at a constant 95 percent. Valid threshold values range from 10 to 94 percent of CPU usage. Valid values for the monitoring period range from 1 to 60 minutes.

Examples

The following example shows how to configure the SNMP CPU threshold level to 75 percent of CPU usage and a monitoring period of 30 minutes:

```
ciscoasa(config)# snmp cpu threshold 75% 30
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP-related traps.

Command	Description
snmp link threshold	Defines the SNMP interface threshold value.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp interface threshold

To configure the threshold value for an SNMP physical interface and the threshold value for system memory usage, use the **snmp interface threshold** command in global configuration mode. To clear the threshold value for an SNMP physical interface and the threshold value for system memory usage, use the **no** form of this command.

snmp interface threshold *threshold_value*
no snmp interface threshold *threshold_value*

Syntax Description

threshold_value	Defines the threshold value as a percentage of CPU usage.

Command Default

If you do not configure the **snmp interface threshold** command, the default threshold value is 70 percent of CPU usage and system memory usage.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(1)	This command was added.

Usage Guidelines

Valid threshold values range from 30 to 99 percent of physical interfaces. The **snmp interface threshold** command is available only in the admin context.

Examples

The following example shows how to configure the SNMP interface threshold value to 75 percent for all physical interfaces:

```
ciscoasa(config)# snmp interface threshold 75%
```

Related Commands

Command	Description
snmp-server enable traps	Enables SNMP-related traps.
snmp cpu threshold rising	Defines the SNMP CPU threshold value.
snmp-server enable	Enables SNMP on the ASA.

Command	Description
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-map

To identify a specific map for defining the parameters for SNMP inspection, use the snmp-map command in global configuration mode. To remove the map, use the **no** form of this command.

snmp-map*map_name*
no snmp-map *map_name*

Syntax Description

map_name	The name of the SNMP map.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the snmp-map command to identify a specific map to use for defining the parameters for SNMP inspection. When you enter this command, the system enters the SNMP map configuration mode, which lets you enter the different commands used for defining the specific map. After defining the SNMP map, you use the inspect snmp command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the inspect command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface.

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enables SNMP application inspection.
policy-map	Associates a class map with specific security actions.

snmp-server community

To set the SNMP community string, use the **snmp-server community** command in global configuration mode. To remove the SNMP community string, use the **no** form of this command.

snmp-server community [**0 | 8**] *community-string*
no snmp-server community [**0 | 8**] *community-string*

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) community string will follow.
8	Specifies that an encrypted community string will follow.
community-string	Sets the SNMP community string, which is the password in encrypted or unencrypted (clear text) format. The community string can have a maximum of 32 characters. **Note** You should avoid the use of special characters (!, @, #, $, %, ^, &, *, \) in community strings. In general, using any special characters reserved for functions used by the operating system can cause unexpected results. For example, the backslash (\) is interpreted as an escape character and should not be used in the community string.

Command Default

The default community string is “public.”

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	The *text* argument was changed to the *community-string* argument.
8.3(1)	Support for encrypted passwords was added.

Usage Guidelines

The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. It is used only for Version 1 and 2c communication between the management station and the device. The ASA uses a key to determine whether or not the incoming SNMP request is valid.

You should avoid the use of special characters (!, @, #, $, %, ^, &, *, \) in community strings. In general, using any special characters reserved for functions used by the operating system can cause unexpected results.

For example, the backslash (\) is interpreted as an escape character and should not be used in the community string.

For example, you could designate a site with a community string and then configure the routers, the ASA, and the management station with this same string. The ASA uses this string and does not respond to requests with an invalid community string.

After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible.

The encrypted community string is always generated by the ASA; you normally enter the clear text form.

Note If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

Examples

The following example sets the community string to ”onceuponatime”:

```
ciscoasa(config)# snmp-server community onceuponatime
```

The following example sets an encrypted community string:

```
ciscoasa(config)# snmp-server community 8 LvAu+JdFG+GjPmZYlKvAhXpb28E=
```

The following example sets an unencrypted community string:

```
ciscoasa(config)# snmp-server community 0 cisco
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP counters.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server contact

To set the SNMP server contact name, use the **snmp-server contact** command in global configuration mode. To remove the SNMP contact name, use the **no** form of this command.

snmp-server contact *text*
no snmp-server contact [*text*]

Syntax Description

text	Specifies the name of the contact person or the ASA system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example sets the SNMP server contact to EmployeeA:

```
ciscoasa(config)# snmp-server contact EmployeeA
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server enable	Enables SNMP on the ASA.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable

To enable the SNMP server on the ASA, use the **snmp-server enable** command in global configuration mode. To disable the SNMP server, use the **no** form of this command.

snmp-server enable
no snmp-server enable

Syntax Description

This command has no arguments or keywords.

Command Default

The SNMP server is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can enable and disable SNMP easily, without configuring and reconfiguring SNMP traps or other configuration.

Examples

The following example enables SNMP, configures the SNMP host and traps, and then sends traps as syslog messages.

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.

Command	Description
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable oid

To enable the ASA to query free memory and used memory statistics through SNMP walk operations, use the **snmp-server enable oid mempool** command in global configuration mode. To disable memory statistic queries, use the **no** form of this command.

snmp-server enable oid mempool
no snmp-server enable oid mempool

Syntax Description

mempool To query free and used memory statistics when you do SNMP walk operations.

The exclusive MIB objects used for **mempool** query include the following:

- ciscoMemoryPoolUsed
- ciscoMemoryPoolFree
- cempMemPoolHCUsed
- cempMemPoolHCFree

Command Default

By default, the **snmp-server enable oid mempool** is enabled to allow SNMP walk operations of these MIB objects.

You can disable these MIB objects using the **no** form of this command. The **clear configure snmp-server** command restores the default enabling of SNMP MIB objects for memory queries.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• No	• Yes	• No

Command History

Release	Modification
9.10(1)	This command was added.

Usage Guidelines

When doing SNMP walk operations, the ASA will query memory information from the MEMPOOL_DMA and MEMPOOL_GLOBAL_SHARED pools. When the ASA queries memory information, the CPU may be held by the SNMP process for too long before releasing the CPU to other processes. This can result in SNMP-related CPU hogs causing packet drops.

To mitigate this issue, avoid polling the OIDs that relate to the Global Shared pool using the **no snmp-server enable oid mempool** command. When disabled, the **mempool** OIDs would return 0 bytes. They can, however, be queried explicitly using a GET request for that pool, irrespective of this command.

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable traps

To enable the ASA to send traps to the NMS, use the **snmp-server enable traps** command in global configuration mode. To disable traps, use the **no** form of this command.

snmp-server enable traps [**all | syslog | snmp** [*trap*] [….] [**cluster-state | failover-state | peer-flap**] [*trap*]] **| config | entity** [*trap*] [….] **| ipsec** [*trap*] [….] **| ikve2** [*trap*] [….] **| remote-access** [*trap*] **| connection-limit-reached | cpu threshold rising | link-threshold | memory-threshold | nat** [*trap*]

no snmp-server enable traps [**all | syslog | snmp** [*trap*] [….] [**cluster-state | failover-state | peer-flap**] [*trap*]] **| config | entity** [*trap*] [….] **| ipsec** [*trap*] [….] [*trap*] [….] **| remote-access** [*trap*] **| connection-limit-reached | cpu threshold rising | link-threshold | memory-threshold | nat** [*trap*]

Syntax Description

all	Enables all traps.
config	Enables configuration traps.
connection-limit-reached	Enables connection limit reached traps.
cpu threshold rising	Enables CPU threshold rising traps.
cluster-state	Enable cluster related traps.
entity [*trap*]	Enables entity traps. Traps for **entity** include the following: • **accelerator-temperature** • **chassis-fan-failure** • **chassis-temperature** • **config-change** • **cpu-temperature** • **fan-failure** • **fru-insert** • **fru-remove** • **l1-bypass-status** • **power-supply** • **power-supply-failure** • **power-supply-presence** • **power-supply-temperature**
failover-state	Enable failover related traps.

ipsec [*trap*]	Enables IPsec traps. Traps for **ipsec** include the following: • **start** • **stop**
ikev2 [*trap*][ ]	Enables IKEv2 IPsec traps. Traps for **ikev2** include: • **start** • **stop**
link-threshold	Enables link threshold reached traps.
memory-threshold	Enables memory threshold reached traps.
nat [*trap*]	Enables NAT-related traps. Traps for **nat** include the following: • **packet-discard**
peer-flap	Enable BGP or OSPF peer MAC address flapping related traps.
remote-access [*trap*]	Enables remote access traps. Traps for **remote-access** include the following: • **session-threshold-exceeded**
snmp [*trap*]	Enables SNMP traps. By default, all SNMP traps are enabled. Traps for **snmp** include the following: • **authentication** • **linkup** • **linkdown** • **coldstart** • warmstart
syslog	Enables syslog message traps.

Command Default

The default configuration has the following **snmp** traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart**). If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.) All other traps are disabled by default.

You can disable these traps using the **no** form of this command with the **snmp** keyword. The **clear configure snmp-server** command restores the default enabling of SNMP traps.

Command Modes

The following table shows the modes in which you can enter the command.

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(1)	The following traps have been added: **snmp warmstart**, **nat packet-discard**, **link-threshold**, **memory-threshold**, **entity power-supply**, **entity fan-failure**, **entity cpu-temperature**, **cpu threshold rising**, and **connection-limit-reached**. These traps do not apply to the ASASM.
8.6(1)	The following traps have been added to support the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X: **entity power-supply-failure**, **entity chassis-fan-failure**, **entity power-supply-presence**, **entity chassis-temperature**, and **entity power-supply-temperature**.
9.0(1)	Support for multiple context mode was added for IKEv2 and IPsec.
9.3(2)	Support for the following traps was added: **config** and **entity accelerator-temperature**.

Usage Guidelines

To enable individual traps or sets of traps, enter this command for each feature type. To enable all traps, enter the **all** keyword.

To send traps to the NMS, enter the **logging history** command, then enable logging using the **logging enable** command.

Traps generated in the admin context only include the following:

- **connection-limit-reached**
- **entity**
- **memory-threshold**

Traps generated through the admin context only for physically connected interfaces in the system context include the following:

- **interface-threshold**

All other traps are available in the admin and user contexts.

The **config** trap enables the ciscoConfigManEvent notification and the ccmCLIRunningConfigChanged notification, which are generated after you have exited configuration mode.

Some traps are not applicable to certain hardware models. Use ? in place of a trap keyword to determine which traps are available for your device. For example:

- The **accelerator-temperature** threshold trap applies only to the ASA 5506-X and ASA 5508-X.
- The **chassis-fan-failure** trap does not apply to the ASA 5506-X.

- The following traps do not apply to the ASA 5506-X and ASA 5508-X: **fan-failure**, **fru-insert**, **fru-remove**, **power-supply**, **power-supply-presence**, and **power-supply-temperature**.
- The Firepower 1000 series, except the 1010, supports the following entity traps only: **chassis-temperature**, **config-change**, and **cpu-temperature**. The 1010 supports the following traps only: **config-change**, **fru-insert**, **fru-remove**.

Multiple Context Mode Guidelines

- In multiple context mode, the **fan-failure** trap, the **power-supply-failure** trap, and the **cpu-temperature** trap are generated only from the admin context, and not the user contexts. These traps apply only to the ASA 5512-X, 5515-X, 5525-X, 5545-X, and 5555-X; they do not apply to the ASA 5505.
- The **snmp-server enable traps remote-access session-threshold-exceeded** command is not supported in multiple context mode.

If the CPU usage is greater than the configured threshold value for the configured monitoring period, a **cpu threshold rising** trap is generated.

When the used system memory reaches 80 percent, the **memory-threshold** trap is generated.

Note SNMP does not monitor voltage sensors.

Examples

The following example enables SNMP, configures the SNMP host and traps, then sends traps as syslog messages:

```
ciscoasa(config)# snmp-server enable
ciscoasa(config)# snmp-server community onceuponatime
ciscoasa(config)# snmp-server location Building 42, Sector 54
ciscoasa(config)# snmp-server contact EmployeeB
ciscoasa(config)# snmp-server host perimeter 10.1.2.42
ciscoasa(config)# snmp-server enable traps all
ciscoasa(config)# logging history 7
ciscoasa(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server group

To configure a new SNMP group, use the **snmp-server group** command in global configuration mode. To remove a specified SNMP group, use the **no** form of this command.

snmp-server group *group-name* { **v3** { **auth | noauth | priv** } }
no snmp-server group *group-name* { **v3** { **auth | noauth | priv** } }

Syntax Description

auth	Specifies packet authentication without encryption.
group-name	Specifies the name of the group.
noauth	Specifies no packet authentication.
priv	Specifies packet authentication with encryption.
v3	Specifies that the group is using the SNMP Version 3 security model, which is the most secure of the supported security models. This version allows you to explicitly configure authentication characteristics.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
8.3(1)	Support for password encryption was added.

Usage Guidelines

To use the Version 3 security model, you must first configure an SNMP group, then configure an SNMP user, and then configure an SNMP host. You must also specify Version 3 and a security level. When a community string is configured internally, two groups with the name “public” are automatically created—one for the Version 1 security model and one for the Version 2c security model. When you delete a community string, both configured groups are automatically deleted.

Note A user that is configured to belong to a certain group should have the same security model as the group.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Note If you downgrade from version 8.3(1) to a lower version of the ASA software and have configured encrypted passwords, you must first revert the encrypted passwords to clear text using the **no key config-key password encryption** command, then save the results.

Examples

The following example show how the ASA can receive SNMP requests using the SNMP Version 3 security model, which includes creating a group, creating a user, and creating a host:

```
ciscoasa(config)#
snmp-server group
 vpn-group
 v3 priv
ciscoasa(config)# snmp-server
 user
 admin vpn-group
v3
 auth sha
 letmein
 priv
 3des
cisco123
ciscoasa(config)# snmp-server host
mgmt 10.0.0.1
version 3
admin
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP configuration counters.
snmp-server host	Sets the SNMP host address.
snmp-server user	Creates a new SNMP user.

snmp-server host

To specify the NMS that can use SNMP on the ASA, use the **snmp-server host** command in global configuration mode. To disable the NMS, use the **no** form of this command.

snmp-server host { *interface* { *hostname* | *ip_address* } } [**trap | poll**] [**community** *0* | *8 community-string*] [**version** { **1 | 2c | 3** *username* }] [**udp-port** *port*]

no snmp-server host { *interface* { *hostname* | *ip_address* } } [**trap | poll**] [**community** *0* | *8 community-string*] [**version** { **1 | 2c | 3** *username* }] [**udp-port** *port*]

Syntax Description

0	(Optional) Specifies that an unencrypted (clear text) community string will follow.
8	Specifies that an encrypted community string will follow.
community	Specifies that a non-default string is required for requests from the NMS, or when generating traps sent to the NMS. Valid only for SNMP Version 1 or 2c.
community-string	Specifies the password-like community string that is sent with the notification or in a request from the NMS. The community string can have a maximum of 32 characters. Can be in encrypted or unencrypted (clear text) format.
hostname	Specifies the SNMP notification host, which is usually an NMS or SNMP manager.
interface	Specifies the interface name through which the NMS communicates with the ASA.
ip_address	Specifies the IP address of an NMS to which SNMP traps should be sent or from which the SNMP requests come.
trap | **poll**	(Optional) Specifies whether the host is allowed to browse (poll) or send traps. If neither is specified, the default is **trap**. Note that both traps and polling cannot be enabled for the same host.
udp-port *port*	(Optional) Specifies that SNMP traps must be sent to an NMS host on a non-default port and sets the UDP port number of the NMS host.
username	Specifies the username to embed in the trap PDU that is sent to the host. Valid only for SNMP Version 3.
version {**1** | **2c** | **3**}	(Optional) Specifies the SNMP version, which is used for traps and requests (polling). The default is 1.

Command Default

The default UDP port is 162.

The default version is 1.

SNMP traps are enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.2(1)	• SNMP Version 3 is supported. • The *username* argument was added. • The *text* argument was changed to the *community-string* argument. • The *interface_name* argument was changed to the *interface* argument.
8.3(1)	Support for encrypted passwords was added.
9.7(1)	If you have a directly-connected SNMP management station, you can use a /31 subnet on the ASA and SNMP server to create a point-to-point connection.
9.8(4)	The SNMP version is now enforced for both traps and polling.
9.9(2)	Support for IPv6 was added.

Usage Guidelines

If you configure the **snmp-server host** command on a port that is currently in use, the following message appears:

```
The UDP port port is in use by another feature.
SNMP requests to the device will fail until the snmp-server listen-port
command is configured to use a different port.
```

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

The default is **trap** if neither [**trap** | **poll**] is specified. It is important to note that for this command, both the traps and polling cannot be enabled for the same host.

To use the Version 3 security model, you must configure an SNMP group first, then an SNMP user, and then an SNMP host. The username must already be configured on the device. When a device is configured as the standby unit of a failover pair, the SNMP engine ID and user configuration are replicated from the active unit. This action allows a transparent switchover from an SNMP Version 3 query perspective. No configuration changes are necessary in the NMS to accommodate a switchover event.

After you have used an encrypted community string, only the encrypted form is visible to all systems (for example, CLI, ASDM, CSM, and so on). The clear text password is not visible.

The encrypted community string is always generated by the ASA; you normally enter the clear text form.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

Examples

The following example sets the host to 192.0.2.5, which is attached to the inside interface:

```
ciscoasa(config)# snmp-server host inside 192.0.2.5
ciscoasa(config)# snmp-server host inside 192.0.2.5
 version 3 username user1 password cisco123 mschap md5aes128 udp-port 190
```

The following examples show how the ASA can receive SNMP requests using the SNMP Version 3 security model, which includes creating a group, creating a user, and creating a host:

```
ciscoasa(config)# snmp-server group vpn-group v3 priv
ciscoasa(config)# snmp-server user admin vpn-group v3
auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3
username user1
```

The following example sets the host to use an encrypted community string:

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 8
LvAu+JdFG+GjPmZYlKvAhXpb28E= username user1 password cisco123 mschap
```

The following example sets the host to use an unencrypted community string:

```
ciscoasa(config)# snmp-server host mgmt 1.2.3.4 community 0
cisco username user1 password cisco123 mschap
```

The following example sets the host to IPv6 address 12:ab:56:ce::11 using SNMP notification version 2c:

```
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11
community public version 2c
```

Related Commands

Command	Description
clear configure snmp-server	Clears SNMP configuration counters.
snmp-server enable	Enables SNMP on the ASA.
snmp-server group	Configures a new SNMP group.
snmp-server user	Configures a new SNMP user.

snmp-server host-group

To associate a single user or a group of users in a user list with a network object, use the **snmp-server host-group** command in global configuration mode. To remove the association, use the **no** form of this command.

snmp-server host-group *interface-network-object-name* [**trap | poll**] [**community** *community-string*] [**version** { **1 | 2c | 3** { *username* **| userlist** *list_name* } }] [**udp-port** *port*]

no snmp-server host-group *interface-network-object-name* [**trap | poll**] [**community** *community-string*] [**version** { **1 | 2c | 3** { *username* **| userlist** *list_name* } }] [**udp-port** *port*]

Syntax Description

community	Specifies that a non-default string is required for requests from the NMS, or when generating traps sent to the NMS. Valid only for SNMP Version 1 or 2c.
community-string	Specifies the password-like community string that is sent with the notification or in a request from the NMS. The community string can have a maximum of 32 characters.
interface-network-object-name	Specifies the interface network object name with which a user or group of users is associated.
trap | **poll**	(Optional) Specifies whether the host is allowed to browse (poll) or send traps. If neither is specified, the default is **poll**. Note that both traps and polling cannot be enabled for the same host group.
udp-port *port*	(Optional) Specifies that SNMP traps must be sent to an NMS host on a non-default port and sets the UDP port number of the NMS host.
user-list *list_name*	Specifies the name of the user list.
username	Specifies the name of the user.
version {**1** | **2c** | **3**}	(Optional) Sets the SNMP notification version to Version 1, 2c, or 3 to use for sending traps.

Command Default

The default UDP port is 162.

The default version is 1.

SNMP polling is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.
9.17(1)	Support for IPv6 objects was added.

Usage Guidelines

You can now add up to 4000 hosts. The number of supported active polling destinations is 128. You can define the hosts using a hostname or a range of IP addresses. You can specify a network object to indicate the individual hosts that you want to add as a host group. You can associate more than one user with one host.

The default is **poll** if [**trap** | **poll**] is not specified. It is important to note that for this command, both the traps and polling cannot be enabled for the same host group. For a mixed monitoring environment where some hosts are configured for polling while others are configured for traps, we recommend that you use the **snmp-server host** command. It is important to note that for the **snmp-server host** command, both the traps and polling cannot be enabled for the same host, and the default is **trap**.

If you are using SNMP notification version 1 or 2c for sending traps, you may associate a single user with a network object. If you are using SNMP notification version 3 for sending traps, you may associate a single user or a group of users with a network object. Use the **snmp-server user-list** command to create a group of users. The users may belong to any group configuration.

If you are using SNMP version 3, you must associate a username with the SNMP host.

Supports IPv4 and IPv6.

Examples

The following example associates a single user with a network object using SNMP notification version 1:

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
```

The following example associates a single user with a network object using SNMP notification version 2c:

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
```

The following example associates a single user with a network object using SNMP notification version 3:

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
```

The following example associates a user list with a network object using SNMP notification version 3:

```
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

Related Commands

Command	Description
clear configure snmp-server host-group	Clears all SNMP host group configurations.
show running-config snmp-server host-group	Filters the SNMP server host group configuration from the running configuration.
snmp-server host	Sets the SNMP host address.

snmp-server listen-port

To set the listening port for SNMP requests, use the **snmp-server listen-port** command in global configuration mode. To restore the default port, use the **no** form of the command.

snmp-server listen-port *lport*
no snmp-server listen-port *lport*

Syntax Description

lport	The port on which incoming requests will be accepted.

Command Default

The default port is 161.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes (admin context only)	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

In multiple context mode, you can use this command in the admin context only. The port applies to all contexts; you cannot use a different port per context.

If you configure the **snmp-server listen-port** command on a port that is currently in use, the following message appears:

```
The UDP port port is in use by another feature.
SNMP requests to the device will fail until the snmp-server listen-port
command is configured to use a different port.
```

The existing SNMP thread continues to poll every 60 seconds until the port is available, and issues syslog message %ASA-1-212001 if the port is still in use.

Examples

The following example sets the listening port to 192:

```
ciscoasa(config)# snmp-server listen-port 192
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server location

To set the ASA location for SNMP, use the **snmp-server location** command in global configuration mode. To remove the location, use the **no** form of this command.

snmp-server location *text*
no snmp-server location [*text*]

Syntax Description

location *text*	Specifies the security appliance location. The **location** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example sets the ASA location for SNMP as Building 42, Sector 54:

```
ciscoasa(config)# snmp-server location Building 42, Sector 54
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the ASA.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.

snmp-server user

To configure a new SNMP user, use the **snmp-server user** command in global configuration mode. To remove a specified SNMP user, use the **no** form of this command.

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** { **sha | sha224 | sha256 | sha384** } *auth_password* [**priv** { **3des | aes** { **128 | 192 | 256** } } *priv_password*]]
no snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** { **sha | sha224 | sha256 | sha384** } *auth_password* [**priv** { **3des | aes** { **128 | 192 | 256** } } *priv_password*]]

Syntax Description

128	(Optional) Specifies the use of the 128-bit AES algorithm for encryption.
192	(Optional) Specifies the use of the 192-bit AES algorithm for encryption.
256	(Optional) Specifies the use of the 256-bit AES algorithm for encryption.
3des	(Optional) Specifies the use of the 168-bit 3DES algorithm for encryption.
aes	(Optional) Specifies the use of the AES algorithm for encryption.
auth	(Optional) Specifies which authentication level should be used.
auth_password	(Optional) Specifies a string that enables the agent to receive packets from the host. The minimum length is one character; the recommended length is at least eight characters, and should include letters and numbers. The maximum length is 64 characters. You can specify a plain-text password or a localized MD5 digest. If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, and cc are hexadecimal values. The digest should be exactly 16 octets long.
engineID	(Optional) Specifies the engineID of the ASA which was used to localize the user's authentication and encryption information. The engineID argument must specify a valid ASA engineID.
encrypted	(Optional) Specifies whether or not the password appears in encrypted format. Encrypted passwords must be in hexadecimal format.
group_name	Specifies the name of the group to which the user belongs.
priv	Specifies packet authentication with encryption.
priv_password	(Optional) Specifies a string that indicates the privacy user password. The minimum length is one character; the recommended length is at least eight characters, and should include letters and numbers. The maximum length is 64 characters. You can specify a plain-text password or a localized MD5 digest. If you have the localized MD5 or SHA digest, you can specify that string instead of the plain-text password. The digest should be formatted as aa:bb:cc:dd, where aa, bb, and cc are hexadecimal values. The digest should be exactly 16 octets long.
sha	(Optional) Specifies the HMAC-SHA-96 authentication level.
sha224	(Optional) Specifies the HMAC-SHA-224 authentication level.

sha256	(Optional) Specifies the HMAC SHA-256 authentication level.
sha384	(Optional) Specifies the HMAC SHA-384 authentication level.
username	Specifies the name of the user on the host that connects to the agent.
v3	Specifies that the SNMP Version 3 security model should be used. Allows the use of the **encrypted, priv,** or **auth** keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.2(1)	This command was added.
9.14(1)	Added the HMAC AES-256 authentication level.
9.16(1)	Added the HMAC AES-224 and AES-384 authentication levels. Removed support for the HMAC-MD5-96 authentication level. Removed support for the 56-bit DES algorithm for encryption.

Usage Guidelines

An SNMP user must be part of an SNMP group. To use the Version 3 security model, you must first configure an SNMP group, then configure an SNMP user, and then configure an SNMP host.

Note If you forget a password, you cannot recover it, and must reconfigure the user.

When the snmp-server user configuration is displayed on the console or written to a file (for example, the startup-configuration file), the localized authentication and privacy digests always appear instead of a plain-text password. This usage is required by RFC 3414, Section 11.2.

Note You must have a 3DES or AES feature license to configure users with the 3DES or AES algorithm.

During bootup or upgrade of the ASA, single-digit passwords and passwords starting with a digit followed by a whitespace are no longer supported. For example, 0 pass and 1 are invalid passwords.

In clustering, you must manually update each clustered ASA with SNMPv3 users. You can do this by entering the **snmp-server user** *username group-name* **v3** command on the master unit with the *priv-password* option and *auth-password* option in their non-localized forms.

An error message appears to inform you that the SNMPv3 user commands will not be replicated during clustering replication or configuration. You may then configure SNMPv3 user and group commands on slave ASAs independently. This also means that existing SNMPv3 user and group commands are not cleared during replication, and you may enter SNMPv3 user and group commands on all slaves in the cluster. For example:

On a master unit using commands entered with keys that have already been localized:

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a priv aes 256
cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

On a slave unit during cluster replication (appears only if an **snmp-server user** commands exist in the configuration):

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

Examples

The following example shows how the ASA can receive SNMP requests using the SNMP Version 3 security model:

```
ciscoasa(config)#
            snmp-server group

engineering


            v3
            auth
ciscoasa(config)# snmp-server
            user

engineering


            v3
            auth sha

mypassword
```

Related Commands

Command	Description
clear configure snmp-server	Clears the SNMP server configuration.
snmp-server enable	Enables SNMP on the ASA.
snmp-server group	Creates a new SNMP group.
snmp-server host	Sets the SNMP host address.

snmp-server user-list

To configure an SNMP user list with a group of specified users in it, use the **snmp-server user-list** command in global configuration mode. To remove a specified SNMP user list, use the **no** form of this command.

snmp-server user-list *list_name* **username** *user_name*
no snmp-server user-list *list_name* **username** *user_name*

Syntax Description

list_name	Specifies the name of the user list, which may be up to 33 characters long.
username *user_name*	Specifies the users who may be configured in the user list.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

You configure the users in the user list with the **snmp-server user** *username* command. The user list must have more than one user in it and can be associated with a hostname or a range of IP addresses.

Examples

The following example shows how to create a group of users for a user list named engineering:

```
ciscoasa(config)#
snmp-server user-list
 engineering username
 user1
ciscoasa(config)# snmp-server
 user-list
 engineering username
 user2
ciscoasa(config)# snmp-server
 user-list
 engineering username
 user3
```

Related Commands

Command	Description
show running-config snmp-server user-list	Filters the SNMP user list configuration from the running configuration.
clear snmp-server user-list	Clears the SNMP user list configuration.

sntp address

To provide the Simple Network Time Protocol (SNTP) server IP address to StateLess Address Auto Configuration (SLAAC) clients when you configure the DHCPv6 server, use the **sntp address** command in ipv6 dhcp pool configuration mode. To remove the SNTP server, use the **no** form of this command.

sntp address *sntp_ipv6_address*
no sntp address *sntp_ipv6_address*

Syntax Description

sntp_ipv6_address	Specifies the SNTP server IPv6 address.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Ipv6 dhcp pool configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

For clients that use SLAAC in conjunction with the Prefix Delegation feature, you can configure the ASA to provide information in an **ipv6 dhcp pool**, including the SNTP server, when they send Information Request (IR) packets to the ASA. The ASA only accepts IR packets, and does not assign addresses to the clients. Configure the DHCPv6 stateless server using the **ipv6 dhcp server** command; you specify an **ipv6 dhcp pool** name when you enable the server.

Configure Prefix Delegation using the **ipv6 dhcp client pd** command.

This feature is not supported in clustering.

Examples

The following example creates two IPv6 DHCP pools, and enables the DHCPv6 server on two interfaces:

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
sntp address 2001:DB8:1::5
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
sntp address 2001:DB8:1::5
```

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

Related Commands

Command	Description
clear ipv6 dhcp statistics	Clears DHCPv6 statistics.
domain-name	Configures the domain name provided to SLAAC clients in responses to IR messages.
dns-server	Configures the DNS server provided to SLAAC clients in responses to IR messages.
import	Uses one or more parameters that the ASA obtained from the DHCPv6 server on the Prefix Delegation client interface, and provides them to SLAAC clients in responses to IR messages.
ipv6 address	Enables IPv6 and configures the IPv6 addresses on an interface.
ipv6 address dhcp	Obtains an address using DHCPv6 for an interface.
ipv6 dhcp client pd	Uses a delegated prefix to set the address for an interface.
ipv6 dhcp client pd hint	Provides one or more hints about the delegated prefix you want to receive.
ipv6 dhcp pool	Creates a pool that includes information that you want to provide to SLAAC clients on a given interface using the DHCPv6 stateless server.
ipv6 dhcp server	Enables the DHCPv6 stateless server.
network	Configures BGP to advertise the delegated prefix received from the server.
nis address	Configures the NIS address provided to SLAAC clients in responses to IR messages.
nis domain-name	Configures the NIS domain name provided to SLAAC clients in responses to IR messages.
nisp address	Configures the NISP address provided to SLAAC clients in responses to IR messages.
nisp domain-name	Configures the NISP domain name provided to SLAAC clients in responses to IR messages.
show bgp ipv6 unicast	Displays entries in the IPv6 BGP routing table.

Command	Description
show ipv6 dhcp	Shows DHCPv6 information.
show ipv6 general-prefix	Shows all the prefixes acquired by the DHCPv6 Prefix Delegation clients and the ASA distribution of that prefix to other processes.
sip address	Configures the SIP address provided to SLAAC clients in responses to IR messages.
sip domain-name	Configures the SIP domain name provided to SLAAC clients in responses to IR messages.
sntp address	Configures the SNTP address provided to SLAAC clients in responses to IR messages.

so – st

software authenticity development

To enable or disable loading development key signed images, use the **software authenticity development** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. Once you enable this option, it persists until you disable loading development key signed images.

software authenticity development { **enable** | **disable** }

Syntax Description

disable	Disables loading development key signed images.
enable	Enables loading development key signed images.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following example shows loading development key signed signatures enabled:

```
ciscoasa(config)# software authenticity development enable
ciscoasa(config)# show software authenticity development
Loading of development images is enabled
ciscoasa(config)#
```

The following example shows loading development key signed images disabled:

```
ciscoasa(config)# software authenticity development disable
ciscoasa(config)# show software authenticity development
Loading of development images is disabled
ciscoasa(config)#
```

Related Commands

Command	Description
show software authenticity keys	Displays the development keys.

Command	Description
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the development key file.
show software authenticity running	Displays the digital signature information related to the current running file.
software authenticity key add special	Adds a new development key to SPI flash.
software authenticity key revoke special	Deletes older development keys from SPI flash.

software authenticity key add special

To add a new development key to the SPI flash, use the **software authenticity key add special** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode.

software authenticity key add special

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following example shows how to add a new development key to SPI flash:

```
ciscoasa(config)# software authenticity key add special
Writing the key to Primary...Success
Writing the key to Backup...Success
Done!
The following example shows what happens if you try to add a new development image to SPR
flash and one already exists:
ciscoasa(config)# software authenticity key add special
Duplicate key found in Primary...Skipping key write
Duplicate key found in Backup...Skipping key write
Done!
```

Related Commands

Command	Description
software authenticity key revoke special	Deletes older development keys from SPI flash.
show software authenticity keys	Displays the development keys in SPI flash.
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the development keys file.

Command	Description
show software authenticity running	Displays the digital signature information related to the current running file.

software authenticity key revoke special

To delete older development keys from SPI flash, use the **software authenticity key revoke special** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode.

software authenticity key revoke special

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.3(2)	This command was added.

Examples

The following example shows how to remove a development key from SPI flash:

```
ciscoasa(config)# software authenticity key revoke special
Revoking the key with version A...Success
Revoking the key with version A...Success
Done!
```

Related Commands

Command	Description
software authenticity key add special	Adds a new development key to SPI flash.
show software authenticity keys	Displays the development keys in SPI flash.
show software authenticity file disk0:asa932-1fbff.SSA	Displays the contents of the development keys file.
show software authenticity running	Displays the digital signature information related to the current running file.

software-version

To identify the Server and User-Agent header fields, which expose the software version of either a server or an endpoint, use the **software-version** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

software-version action { **mask | log** } [**log**]

no software-version action { **mask | log** } [**log**]

Syntax Description

log	Specifies standalone or additional log in case of violation.
mask	Masks the software version in the SIP message.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to identify the software version in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# software-version action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

source-interface

To specify the source interface name for the VXLAN VTEP interface, use the **source-interface** command in nve configuration mode. To remove the interface, use the **no** form of this command.

source-interface*interface_name*
no source-interface *interface_name*

Syntax Description

interface_name	Sets the VTEP source interface name.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nve configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

The VTEP source interface is a regular ASA interface (physical, redundant, EtherChannel, or even VLAN) with which you plan to associate all VNI interfaces. You can configure one VTEP source interface per ASA/security context.

The VTEP source interface can be devoted wholly to VXLAN traffic, although it is not restricted to that use. If desired, you can use the interface for regular traffic and apply a security policy to the interface for that traffic. For VXLAN traffic, however, all security policy must be applied to the VNI interfaces. The VTEP interface serves as a physical port only.

In transparent firewall mode, the VTEP source interface is not part of a BVI, and you do configure an IP address for it, similar to the way the management interface is treated.

Note If the source interface MTU is less than 1554 bytes, then the ASA automatically raises the MTU to 1554 bytes.

Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

Related Commands

Command	Description
debug vxlan	Debugs VXLAN traffic.
default-mcast-group	Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface.
encapsulation vxlan	Sets the NVE instance to VXLAN encapsulation.
inspect vxlan	Enforces compliance with the standard VXLAN header format.
interface vni	Creates the VNI interface for VXLAN tagging.
mcast-group	Sets the multicast group address for the VNI interface.
nve	Specifies the Network Virtualization Endpoint instance.
nve-only	Specifies that the VXLAN source interface is NVE-only.
peer ip	Manually specifies the peer VTEP IP address.
segment-id	Specifies the VXLAN segment ID for a VNI interface.
show arp vtep-mapping	Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses.
show interface vni	Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with.
show mac-address-table vtep-mapping	Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses.
show nve	Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface.
show vni vlan-mapping	Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode.
source-interface	Specifies the VTEP source interface.
vtep-nve	Associates a VNI interface with the VTEP source interface.
vxlan port	Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789.

speed

To set the speed of an interface, use the **speed** command in interface configuration mode. To restore the speed setting to the default, use the **no** form of this command.

speed { *speed* | **auto** | **nonegotiate** | **sfp-detect** }
no speed [*speed* | **auto** | **nonegotiate** | **sfp-detect**]

Syntax Description

auto	Auto detects the speed. RJ-45 only.
nonegotiate	For SFP interfaces (except for the Secure Firewall 3100), **no speed nonegotiate** sets the speed to 1000 Mbps and enables link negotiation for flow-control parameters and remote fault information. For 10 Gbps interfaces, this option sets the speed down to 1000 Mbps. The **nonegotiate** keyword is the only keyword available for SFP interfaces. The **speed nonegotiate** command disables link negotiation. For the Secure Firewall 3100, see the **negotiate-auto** command.
speed	Sets the speed to a specific setting.
sfp-detect	(Secure Firewall 3100 only) Detects the speed of the installed SFP module and uses the appropriate speed. Duplex is always full, and auto-negotiation is always enabled. This option is useful if you later change the network module to a different model, and want the speed to update automatically. This setting is the default.

Command Default

For RJ-45 interfaces, the default is **speed auto**.

For SFP interfaces (except for the Secure Firewall 3100), the default is **no speed nonegotiate**.

For the Secure Firewall 3100, the default is **sfp-detect**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.
9.14(1)	Speed auto-negotation can be disabled on 1GB fiber interfaces on the Firepower 1000 and 2100 using the **speed nonegotiate** command.
9.17(1)	We added the sfp-detect keyword for the Secure Firewall 3100.

Usage Guidelines

Set the speed on the physical interface only.

If your network does not support auto detection, set the speed to a specific value.

For RJ-45 interfaces on the ASA 5500 series, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the speed to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Note Do not set the **speed** command for an ASA 5500-X or an ASA 5585-X with fiber interfaces. Doing so causes a link failure.

Examples

The following example sets the speed to 1000BASE-T:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
duplex	Sets the duplex mode.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.

spf-interval

To customize IS-IS throttling of shortest path first (SPF) calculations, use the **spf-interval** command in router isis configuration mode. To restore the default values, use the **no** form of this command.

spf-interval [**level-1 | level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]
no spf-interval [**level-1 | level-2**] *spf-max-wait* [*spf-initial-wait spf-second-wait*]

Syntax Description

level-1	(Optional) Apply intervals to Level-1 areas only.
level-2	(Optional) Apply intervals to Level-2 areas only.
spf-max-wait	Indicates the maximum interval (in seconds) between two consecutive SPF calculations. The range is from 1 to 120 seconds. The default is 10 seconds.
spf-initial-wait	(Optional) Indicates the initial SPF calculation delay (in milliseconds) after a topology change. The range is from 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).
spf-second-wait	(Optional) Indicates the hold time between the first and second SPF calculation (in milliseconds). The range is from 1 to 120000 milliseconds. The default is 5500 milliseconds (5.5 seconds).

Command Default

spf-max-wait —10 seconds

spf-initial-wait —5500 milliseconds

spf-second-wait —5500 milliseconds

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

SPF calculations are performed only when the topology changes. They are not performed when external routes change.

The **spf-interval** command controls how often the software performs the SPF calculation. The SPF calculation is processor-intensive. Therefore, it may be useful to limit how often the calculation is done, especially when the area is large and the topology changes often. Increasing the SPF interval reduces the processor load of the router, but potentially slows down the rate of convergence.

The following description will help you determine whether to change the default values of this command:

- The *spf-initial-wait* argument indicates the initial wait time (in milliseconds) after a topology change before the first SPF calculation.
- The *spf-second-wait* argument indicates the interval (in milliseconds) between the first and second SPF calculation.
- Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the *spf-max-wait* interval specified; the SPF calculations are throttled or slowed down after the initial and second intervals. Once the *spf-max-wait* interval is reached, the wait interval continues at this interval until the network calms down.
- After the network calms down and there are no triggers for 2 times the *spf-max-wait* interval, fast behavior is restored (the initial wait time).

SPF throttling is not a dampening mechanism; that is, SPF throttling does not prevent SPF calculations or mark any route, interface, or router as down. SPF throttling simply increases the intervals between SPF calculations.

Examples

The following example configures intervals for SPF calculations, partial route calculation (PRC), and link-state packet (LSP) generation:

```
ciscoasa(config)# router isis
ciscoasa(config-router)# spf-interval 5 10 20
ciscoasa(config-router)# prc-interval 5 10 20
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.

Command	Description
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.

Command	Description
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

split-dns

To enter a list of domains to be resolved through the split tunnel, use the **split-dns** command in group-policy configuration mode. To delete a list, use the **no** form of this command.

To delete all split tunneling domain lists, use the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns none** command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, use the **split-dns none** command.

split-dns { **value** *domain-name1 domain-name2 domain-nameN* **|** **none** }
no split-dns [*domain-name1 domain-name2 domain-nameN*]

Syntax Description

value *domain-name*	Provides a domain name that the ASA resolves through the split tunnel.
none	Indicates that there is no split DNS list. Sets a split DNS list with a null value, thereby disallowing a split DNS list. Prevents inheriting a split DNS list from a default or specified group policy.

Command Default

Split DNS is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 492 characters. You can use only alphanumeric characters, hyphens (-), and periods (.).

The **no split-dns** command, when used without arguments, deletes all current values, including a null value created by issuing the **split-dns none** command.

Starting with version 3.0.4235, Secure Client supports true split DNS functionality for Windows platforms.

Examples

The following example shows how to configure the domains Domain1, Domain2, Domain3 and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that the IPsec client uses the for DNS queries which omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the ASA uses to distinguish which networks require tunneling.
split-tunnel-policy	Lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in cleartext form

split-horizon

To reenable EIGRP split horizon, use the **split-horizon** command in interface configuration mode. To disable EIGRP split horizon, use the **no** form of this command.

split-horizon eigrp *as-number*
no split-horizon eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.

Command Default

The **split-horizon** command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

For networks that include links over X.25 packet-switched networks, you can use the **neighbor** command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

In general, it is best that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. If split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables EIGRP split horizon on interface Ethernet0/0:

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# no split-horizon eigrp 100
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

split-tunnel-all-dns

To enable the Secure Client to the resolve all DNS addresses through the VPN tunnel, use the split-tunnel-all-dns command from group policy configuration mode.

To remove the command from the running configuration, use the no form of this command. This enables inheritance of the value from another group policy.

split-tunnel-all-dns { **disable | enable** }
no split-tunnel-all-dns [{ **disable | enable** }]

Syntax Description

disable (default)	The Secure Client sends DNS queries over the tunnel according to the split tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list.
enable	The Secure Client resolves all DNS addresses through the VPN tunnel.

Command Default

The default is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.2(5)	This command was added.

Usage Guidelines

The split-tunnel-all-dns enable command applies to VPN connections using the SSL or IPsec/IKEv2 protocol, and instructs the Secure Client to resolve all DNS addresses through the VPN tunnel. If DNS resolution fails, the address remains unresolved and the Secure Client does not try to resolve the address through public DNS servers.

By default, this feature is disabled. The client sends DNS queries over the tunnel according to the split tunnel policy—tunnel all networks, tunnel networks specified in a network list, or exclude networks specified in a network list.

Examples

The following example configures the ASA to enable the Secure Client to resolve all DNS queries through the VPN tunnel:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-all-dns enable
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that the legacy IPsec (IKEv1) VPN client or the AnyConnect VPN Client (SSL) uses for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets a legacy VPN client (IPsec/IKEv1) or the AnyConnect VPN client (SSL) conditionally direct packets over a tunnel in encrypted form, or to a network interface in clear text form

split-tunnel-network-list

To create a network list for split tunneling, use the **split-tunnel-network-list** command in group-policy configuration mode. To delete a network list, use the **no** form of this command.

split-tunnel-network-list { **value** *access-list name* | **none** }
no split-tunnel-network-list value [*access-list name*]

Syntax Description

none	Indicates that there is no network list for split tunneling; the ASA tunnels all traffic. Sets a split tunneling network list with a null value, thereby disallowing split tunneling. Prevents inheriting a default split tunneling network list from a default or specified group policy.
value *access-list name*	Identifies an access list that enumerates the networks to tunnel or not tunnel.

Command Default

By default, there are no split tunneling network lists.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA makes split tunneling decisions on the basis of a network list, which is a standard ACL that consists of a list of addresses on the private network. Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, use the **split-tunnel-network-list none** command.

To delete all split tunneling network lists, use the **no split-tunnel-network-list** command without arguments. This deletes all configured network lists, including a null list created by issuing the **split-tunnel-network-list none** command.

Note Starting with version 9.7(1), you can specify up to 1200 split networks. In prior releases, the limit is 200 networks.

Examples

The following example shows how to set a network list called FirstList for the group policy named FirstGroup:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# split-tunnel-network-list value FirstList
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
default-domain	Specifies a default domain name that he IPsec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-policy	Lets an IPsec client conditionally direct packets over an IPsec tunnel in encrypted form, or to a network interface in cleartext form.

split-tunnel-policy

To set a split tunneling policy, use the **split-tunnel-policy** command in group-policy configuration mode. To remove the split-tunnel-policy attribute from the running configuration, use the **no** form of this command.

split-tunnel-policy { **tunnelall | tunnelspecified | excludespecified** }
no split-tunnel-policy

Syntax Description

excludespecified	Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. This option works with Secure Client only.
split-tunnel-policy	Indicates that you are setting rules for tunneling traffic.
tunnelall	Specifies that no traffic goes in the clear or to any other destination than the ASA. Remote users reach Internet networks through the corporate network and do not have access to local networks.
tunnelspecified	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the remote user's Internet service provider.

Command Default

Split tunneling is disabled by default, which is **tunnelall**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable split tunneling.

This enables inheritance of a value for split tunneling from another group policy.

Split tunneling lets a remote-access VPN client conditionally direct packets over an IPsec or SSL tunnel in encrypted form, or to a network interface in cleartext form. With split-tunneling enabled, packets not bound for destinations on the other side of the IPsec or SSL VPN tunnel endpoint do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 split-tunnel-policy tunnelspecified
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPsec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list none	Indicates that no access list exists for split tunneling. All traffic travels across the tunnel.
split-tunnel-network-list value	Identifies the access list the ASA uses to distinguish networks that require tunneling and those that do not.

spoof-server

To substitute a string for the server header field for HTTP protocol inspection, use the **spoof-server** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

spoof-server*string*
no spoof-server *string*

Syntax Description

string	String to substitute for the server header field. 82 characters maximum.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

WebVPN streams are not subject to the spoof-server comand.

Examples

The following example shows how to substitute a string for the server header field in an HTTP inspection policy map:

```
ciscoasa(config-pmap-p)# spoof-server
string
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

sq-period

To specify the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture, use the **sq-period** command in nac-policy-nac-framework configuration mode. To remove the command from the NAC policy, use the **no** form of this command.

sq-period *seconds*
no sq-period [*seconds*]

Syntax Description

seconds	Number of seconds between each successful posture validation. The range is 30 to 1800.

Command Default

The default value is 300.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Nac-policy-nac-framework configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.3(0)	"nac-" removed from command name. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was added.

Usage Guidelines

The ASA starts the status query timer after each successful posture validation and status query response. The expiration of this timer triggers a query for changes in the host posture, referred to as a *status query* .

Examples

The following example changes the value of the status query timer to 1800 seconds:

```
ciscoasa(config-nac-policy-nac-framework)# sq-period 1800
ciscoasa(config-nac-policy-nac-framework)
```

The following example removes the status query timer from the NAC Framework policy:

```
ciscoasa(config-nac-policy-nac-framework)# no sq-period
ciscoasa(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.

Command	Description
nac-settings	Assigns a NAC policy to a group policy.
eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
debug eap	Enables logging of Extensible Authentication Protocol events to debug NAC Framework messaging.

srv-id

To configure a uri-id in a reference-identity object, use the **uri-id** command in ca-reference-identity mode. To delete a uri-id in, use the **no** form of this command. You can access the *ca-reference-identity* mode by first entering the **crypto ca reference-identity** command to configure a reference-identity object..

srv-id*value*
no srv-id *value*

Syntax Description

value	Value of each reference-id.
srv-id	A subjectAltName entry of type otherName whose name form is SRVName as defined in RFC 4985. A SRV-ID identifier may contain both a domain name and an application service type. For example, a SRV-ID of "_imaps.example.net" would be split into a DNS domain name portion of "example.net" and an application service type portion of "imaps."

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
ca-reference-identity	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Once a reference identity has been created, the four identifier types and their associated values can be added or deleted from the reference identity.

The reference identifiers MAY contain information identifying the application service and MUST contain information identifying the DNS domain name.

Examples

The following example creates a reference-identity for a syslog server:

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

Related Commands

Command	Description
crypto ca reference-identity	Configures a reference identity object.

Command	Description
cn-id	Configures a Common Name Identifier in the reference-identity object.
dns-id	Configures and DNS domain name Identifier in a reference identity object.
uri-id	Configures a URI identifier in a reference identity object.
logging host	Configures a logging server that can use a reference-identity object for a secure connection.
call-home profile destination address http	Configures a Smart Call Home server that can use a reference-identity object for a secure connection.

ss7 variant

To identify the SS7 variant used in your network for M3UA inspection, use the **ss7 variant** command in parameters configuration mode. You can access the parameters configuration mode by first entering the **policy-map type inspect m3ua** command. Use the **no** form of this command to return to the default SS7 variant.

ss7 variant { **ITU | ANSI | Japan | China** }
no ss7 variant { **ITU | ANSI | Japan | China** }

Syntax Description

ITU	The ITU variant. This is the default.
ANSI	The ANSI variant.
Japan	The Japan variant.
China	The China variant.

Command Default

The default is the ITU SS7 variant.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(2)	This command was added.

Usage Guidelines

Use this command to identify the SS7 variant used in your network. After you configure the option and deploy an M3UA policy, you cannot change it unless you first remove the policy.

The variant determines the format of the point codes used in M3UA messages.

- ITU—Point codes are 14 bit in 3-8-3 format. The value ranges are [0-7]-[0-255]-[0-7]. This is the default SS7 variant.
- ANSI—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].
- Japan—Point codes are 16 bit in 5-4-7 format. The value ranges are [0-31]-[0-15]-[0-127].
- China—Point codes are 24 bit in 8-8-8 format. The value ranges are [0-255]-[0-255]-[0-255].

Examples

The following example sets the SS7 variant to ITU.

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.
match dpc	Matches the M3UA destination point code.
match opc	Matches the M3UA originating point code.
policy-map type inspect	Creates an inspection policy map.

ssh

To add SSH access to the ASA, use the **ssh** command in global configuration mode. To disable SSH access to the ASA, use the **no** form of this command.

ssh { *ip_address mask* | *ipv6_address/prefix* } *interface*
no ssh { *ip_address mask* | *ipv6_address/prefix* } *interface*

Syntax Description

interface	The ASA interface on which SSH is enabled. Specify any named interface. For bridge groups, specify the bridge group member interface. For VPN management access only (see the **management-access** command), specify the named BVI interface.
ip_address	IPv4 address of the host or network authorized to initiate an SSH connection to the ASA.
ipv6_address/prefix	The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the ASA.
mask	Network mask for *ip_address*.

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
8.4(2)	You can no longer connect to the ASA using SSH with the **pix** or **asa** username and the login password. To use SSH, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command (CLI) or **Configuration > Device Management > Users/AAA > AAA Access > Authentication** (ASDM); then define a local user by entering the **username** command (CLI) or choosing **Configuration > Device Management > Users/AAA > User Accounts** (ASDM). If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.
8.4(4.1), 9.1(2)	You can enable public key authentication for SSH connections to the ASA on a per-user basis with the **ssh authentication** command.

Release	Modification
9.1(2)	The SSH server implementation in the ASA now supports AES-CTR mode encryption.
9.1(7)/9.4(3)/9.5(3)/9.6(1)	You can configure encryption and integrity ciphers for SSH access using the **ssh cipher encryption** and **ssh cipher integrity** commands.
9.6(2)	The **aaa authentication ssh console LOCAL** command is required for **ssh authentication**. In Version 9.6(2) and later, you can create a **username** without any password defined, so you can require public key authentication only.
9.7(1)	If you have a directly-connected SSH management station, you can use a /31 subnet on the ASA and the host to create a point-to-point connection.
9.6(3)/9.8(1)	Separate authentication for users with SSH public key authentication and users with passwords. You no longer have to explicitly enable AAA SSH authentication (**aaa authentication ssh console)**; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with passwords, and you can use any AAA server type.
9.9(2)	Virtual interfaces can now be specified.

Usage Guidelines

The ssh *ip_address* command specifies hosts or networks that are authorized to initiate an SSH connection to the ASA. You can have multiple **ssh** commands in the configuration.

Before you can begin using SSH to the ASA, you must generate a default RSA key using the **crypto key generate rsa** command.

To access the ASA interface for SSH access, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

SSH access to an interface other than the one from which you entered the ASA is not supported. For example, if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface. The only exception to this rule is through a VPN connection (see the **management-access** command).

The ASA allows a maximum of 5 concurrent SSH connections per context/single mode, with a maximum of 100 connections divided among all contexts.

The ASA supports the SSH remote shell functionality provided in SSH Version 2 and supports DES and 3DES ciphers.

The following SSH Version 2 features are not supported on the ASA:

- X11 forwarding
- Port forwarding
- SFTP support
- Kerberos and AFS ticket passing
- Data compression

To use SSH with a username and password, you must configure AAA authentication using the **aaa authentication ssh console LOCAL** command; then define a local user by entering the **username** command. If you want to use a AAA server for authentication instead of the local database, we recommend also configuring local authentication as a backup method.

To use SSH with a local **username** and public key authentication, configure the **ssh authentication** command. Only the local database is supported.

In Version 9.6(2) and 9.7(1), the **aaa authentication ssh console LOCAL** command is required for **ssh authentication**. In Version 9.6(2) and later, you can create a **username** without any password defined, so you can require public key authentication only.

Note Do not use the **username** command **nopassword** option to avoid having to create a username with a password; the **nopassword** option allows *any* password to be entered, not no password. If you configure the **aaa** command, then the **nopassword** option creates a security problem.

For 9.6(1) and earlier and for 9.6(3)/9.8(1) and later, you do not have to configure the **aaa authentication ssh console LOCAL** command; this command only applies to users with passwords, and you can specify any server type, not just LOCAL. For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS. If you do configure the **aaa authentication ssh console LOCAL** command, you can choose to log in with either the **username** password, or with the private key.

Examples

The following example shows how to generate RSA keys and let a host on the inside interface with an address of 192.168.1.2 access the ASA:

```
ciscoasa(config)# crypto key generate rsa modulus 1024
ciscoasa(config)# write memory
ciscoasa(config)# aaa authentication ssh console LOCAL

WARNING: local database is empty! Use 'username' command to define local users.
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
ciscoasa(config)# ssh timeout 30
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
crypto key generate rsa	Generates RSA key pairs for identity certificates.
debug ssh	Displays debugging information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh scopy enable	Enables a secure copy server on the ASA.
ssh version	Restricts the ASA to using either SSH Version 1 or SSH Version 2.

ssh authentication

To enable SSH public key authentication on a per-user basis, use the **ssh authentication** command in username attributes mode. To disable public key authentication on a per-user basis, use the **no** form of this command.

ssh authentication { **pkf | publickey** [**nointeractive**] *key* [**hashed**] }
no ssh authentication { **pkf | publickey** [**nointeractive**] *key* [**hashed**] }

Syntax Description

hashed	When you view the key on the ASA using the **show running-config username** command, the key is encrypted using a SHA-256 hash. Even if you entered the key as **pkf** , the ASA hashes the key, and shows it as a hashed **publickey** . If you need to copy the key from **show** output, specify the **publickey** type with the **hashed** keyword.
key	The value of the key argument can be one of the following: • When the key argument is supplied and the hashed tag is not specified, the value of the key must be a Base 64 encoded public key that is generated by SSH key generation software that can generate ssh-rsa, ecdsa-sha2-nistp, or ssh-ed25519 raw keys (that is, with no certificates). After you submit the Base 64 encoded public key, that key is then hashed via SHA-256 and the corresponding 32-byte hash is used for all further comparisons. • When the key argument is supplied and the hashed tag is specified, the value of the key must have been previously hashed with SHA-256 and be 32 bytes long, with each byte separated by a colon (for parsing purposes).
nointeractive	The **nointeractive** option suppresses all prompts when importing an SSH public key file formatted key. This noninteractive data entry mode is only intended for ASDM use.
pkf	For a **pkf** key, you are prompted to paste in a PKF formatted key, up to 4096 bits. Use this format for keys that are too large to paste inline in Base64 format. For example, you can generate a 4096-bit key using ssh keygen, then convert it to PKF, and use the **pkf** keyword to be prompted for the key. **Note** You can use the **pkf** option with failover, but the PKF key is not automatically replicated to the standby system. You must enter the **write standby** command to synchronize the PKF key.
publickey	For a **publickey** , the *key* is a Base64-encoded public key. You can generate the key using any SSH key generation software (such as ssh keygen) that can generate SSH-RSA raw keys (with no certificates).

Command Default

No default behaviors or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username attributes	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(4.1), 9.1(2)	This command was added. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*
9.1(2)	We added the **pkf** keyword and support for keys up to 4096-bits.
9.6(2)	The **aaa authentication ssh console LOCAL** command is required for **ssh authentication** . In Version 9.6(2) and later, you can create a **username** without any password defined, so you can require public key authentication only.
9.6(3)/9.8(1)	Separate authentication for users with SSH public key authentication and users with passwords. You no longer have to explicitly enable AAA SSH authentication (**aaa authentication ssh console)** ; when you configure the **ssh authentication** command for a user, local authentication is enabled by default for users with this type of authentication. Moreover, when you explicitly configure AAA SSH authentication, this configuration only applies for usernames with passwords, and you can use any AAA server type.
9.16(1)	Support for EdDSA and ECDSA keys was added.

Usage Guidelines

For a local **username** , you can enable public key authentication instead of password authentication. You can generate a public key/private key pair using any SSH key generation software (such as ssh keygen) that can generate ssh-rsa, ecdsa-sha2-nistp, or ssh-ed25519 raw keys (with no certificates). Use the **ssh authentication** command to enter the public key on the ASA. The SSH client then uses the private key (and the passphrase you used to create the key pair) to connect to the ASA.

Only the local database is supported.

When you save the configuration, the hashed key value is saved to the configuration and used when the ASA is rebooted.

In Version 9.6(2) and 9.7(1), the **aaa authentication ssh console LOCAL** command is required for **ssh authentication** . In Version 9.6(2) and later, you can create a **username** without any password defined, so you can require public key authentication only.

Note Do not use the **username** command **nopassword** option to avoid having to create a username with a password; the **nopassword** option allows *any* password to be entered, not no password. If you configure the **aaa** command, then the **nopassword** option creates a security problem.

For 9.6(1) and earlier and for 9.6(3)/9.8(1) and later, you do not have to configure the **aaa authentication ssh console LOCAL** command; this command only applies to users with passwords, and you can specify any server type, not just LOCAL. For example, some users can use public key authentication using the local database, and other users can use passwords with RADIUS. If you do configure the **aaa authentication ssh console LOCAL** command, you can choose to log in with either the **username** password, or with the private key.

Examples

The following example shows how to authenticate using a PKF formatted key:

```
ciscoasa(config)# crypto key generate eddsa edwards-curve ed25519
ciscoasa(config)# write memory
ciscoasa(config)# username deanwinchester password examplepassword1 privilege 15
ciscoasa(config)# username deanwinchester attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config-username)# aaa authentication ssh console LOCAL
ciscoasa(config)# ssh 192.168.1.2 255.255.255.255 inside
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debugging information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh version	Restricts the ASA to using either SSH Version 1 or SSH Version 2.

ssh cipher encryption

Users can select encryption and integrity algorithms when configuring SSH access. For fine grain control over the SSH cipher encryption algorithms, use the **ssh cipher encryption** command in global configuration mode. Predefined levels are available, which correspond to particular sets of algorithms. Also, you can define a custom list by specifying multiple colon-delimited algorithms. To restore the default, use the **no** form of this command.

ssh cipher encryption { **all** | **fips** | **high** | **low** | **medium** | **custom** *encryption_1* [**:** *encryption_2* [**:** *...encryption_n*]] }
no ssh cipher encryption { **all** | **fips** | **high** | **low** | **medium** | **custom** *encryption_1* [**:** *encryption_2* [**:** *...encryption_n*]] }

Syntax Description

all	Specifies that all encryption algorithms are accepted.
custom *encryption_1* [**:** *encryption_2* [**:** ... *encryption_n*]]	Specifies a custom set of encryption algorithms. Enter the **show ssh ciphers** command to view all available encryption algorithms. For example: **custom 3des-cbc:aes192-cbc:aes256-ctr**
fips	Specifies only FIPS-compliant encryption algorithms
high	Specifies only high strength encryption algorithms.
low	Specifies low, medium, and high strength encryption algorithms.
medium	Specifies the medium and high strength encryption algorithms.

Command Default

Medium is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(7)/9.4(3)/9.5(3)/9.6(1)	This command was added.
9.16(1)	We added the **chacha20-poly1305@openssh.com** and **aes128-gcm@openssh.com** algorithms.

Usage Guidelines

This command is used with the **ssh cipher integrity** command. For encryption algorithms, the following values are possible:

- all—3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes192-ctr aes256-ctr
- fips—aes128-cbc aes256-cbc aes128-gcm@openssh.com
- high—aes256-cbc aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr
- low—3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr
- medium—3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr

Note If FIPS mode is enabled, then only the FIPS encryption and integrity algorithms are allowed.

Optionally, some of the algorithms can be deselected. When FIPS mode is enabled, the intersection of the currently configured algorithms and the FIPS-compliant algorithms is calculated. If not NULL, the resulting configuration is used. If NULL, then the default FIPS-compliant algorithms are used.

The performance of secure copy depends partly on the encryption cipher used. If you choose the medium cipher set, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use the **ssh cipher encryption** command; for example, **ssh cipher encryption custom aes128-cbc** .

Examples

The following example shows the configuration of some custom SSH encryption algorithms:

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

Related Commands

Command	Description
show ssh	Displays the configured ciphers.
show ssh ciphers	Displays the available cipher algorithms.
ssh cipher integrity	Specifies configured SSH cipher integrity algorithms.

ssh cipher integrity

Users can select encryption and integrity cipher modes when configuring SSH access. For fine grain control over the SSH cipher integrity algorithms, use the **ssh cipher integrity** command in global configuration mode. Pre-defined levels are available, which correspond to particular sets of algorithms. Also, a custom list can be defined by specifying multiple colon delimited algorithms. To restore the default, use the **no** form of this command.

ssh cipher integrity { **all** | **fips** | **high** | **low** | **medium** | **custom** *algorithm_1* [**:** *algorithm_2* [**:** *...algorithm_n*]] }

no ssh cipher integrity { **all** | **fips** | **high** | **low** | **medium** | **custom** *algorithm_1* [**:** *algorithm_2* [**:** *...algorithm_n*]] }

Syntax Description

all	Specifies that all integrity algorithms are accepted.
custom *algorithm_1*[**:***algorithm_2*[**:***...algorithm_n*]]	Specifies a custom set of integrity algorithms. Enter the **show ssh ciphers** command to view all available integrity algorithms. For example: **custom hmac-sha1:hmac-sha1-96:hmac-md5-96**
fips	Specifies only FIPS-compliant integrity algorithms
high	Specifies only high strength integrity algorithms.
low	Specifies low, medium, and high strength integrity algorithms.
medium	Specifies the medium and high strength integrity algorithms.

Command Default

(9.12 and later) High is the default.

(9.10 and earlier) Medium is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.1(7)/9.4(3)/9.5(3)/9.6(1)	This command was added.

Release	Modification
9.12(1)	We added HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha1 and hmac-sha2-256). The former default was the medium set.
9.13(1)	The following values of integrity algorithms are considered as insecure and deprecated: • all —hmac-sha1-96, hmac-md5, hmac-md5-96, hmac-sha2-256 • low — hmac-sha1-96 , hmac-md5, hmac-md5-96, hmac-sha2-256 • medium— hmac-sha1-96 The above values will be removed from later release.

Usage Guidelines

This command is used with the **ssh cipher encryption** command. For integrity algorithms, the following values are possible:

- all—hmac-sha1, hmac-sha1-96(Deprecated), hmac-md5(Deprecated), hmac-md5-96(Deprecated), hmac-sha2-256(Deprecated)
- fips—hmac-sha1, hmac-sha2-256
- high—hmac-sha1, hmac-sha2-256
- low—hmac-sha1, hmac-sha1-96(Deprecated), hmac-md5(Deprecated), hmac-md5-96(Deprecated), hmac-sha2-256(Deprecated)
- medium—hmac-sha1, hmac-sha1-96(Deprecated), hmac-md5, hmac-md5-96, hmac-sha2-256

Note If FIPS mode is enabled, then only the FIPS encryption and integrity algorithms are allowed.

Optionally, some of the algorithms can be deselected. When FIPS mode is enabled, the intersection of the currently configured algorithms and the FIPS-compliant algorithms is calculated. If not NULL, the resulting configuration is used. If NULL, then the default FIPS-compliant algorithms are used.

Examples

The following example shows the configuration of some custom SSH integrity algorithms:

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

Related Commands

Command	Description
show ssh	Displays the configured ciphers.
show ssh ciphers	Displays the available cipher algorithms.
ssh cipher encryption	Specifies configured SSH cipher encryption algorithms.

ssh disconnect

To disconnect an active SSH session, use the **ssh disconnect** command in privileged EXEC mode.

ssh disconnect *session_id*

Syntax Description

session_id	Disconnects the SSH session specified by the ID number.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You must specify a session ID. Use the **show ssh sessions** command to obtain the ID of the SSH session you want to disconnect.

Examples

The following example shows an SSH session being disconnected:

```
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State          Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
ciscoasa# ssh disconnect 2
ciscoasa# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State          Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

Related Commands

Command	Description
show ssh sessions	Displays information about active SSH sessions to the ASA.

Command	Description
ssh timeout	Sets the timeout value for idle SSH sessions.

ssh key-exchange group

To set the SSH key exchange method, use the **ssh key-exchange group** command in global configuration mode. To restore the default, use the **no** form of this command.

ssh key-exchange group { **curve25519-sha256** | **dh-group14-sha1** | **dh-group14-sha256** | **ecdh-sha2-nistp256** }
no ssh key-exchange group

Syntax Description

curve25519-sha256	Uses Elliptic Curve 25519 SHA256 for the key exchange.
dh-group14-sha1	Uses Diffie-Hellman Group 14 SHA1 for the key exchange.
dh-group14-sha256	(Default) Uses Diffie-Hellman Group 14 SHA256 for the key exchange.
ecdh-sha2-nistp256	Uses Elliptic Curve Diffie-Hellman (ECDH) SHA2 NIST P-256 for the key exchange.

Command Default

(9.12 and later) By default, **dh-group14-sha256** is used.

(9.10 and earlier) By default, the **dh-group1-sha1** is used.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes (Admin context only)	—

Command History

Release	Modification
9.16(1)	We added the **curve25519-sha256** and **ecdh-sha2-nistp256** options.
9.13(1)	The **dh-group1-sha1** option was deprecated and will be removed in a later release.
9.12(2)	Setting the SSH key exchange mode is restricted to the Admin context in multiple context mode.
9.12(1)	We added the **dh-group14-sha256** option, which is also now the default.
8.4(4.1), 9.1(2)	We introduced this command. *This feature is not available in 8.5(1), 8.6(1), 8.7(1), 9.0(1), 9.0(2), or 9.1(1).*

Usage Guidelines

A key exchanges like Diffie-Hellman (DH) provides a shared secret that cannot be determined by either party alone. The key exchange is combined with a signature and the host key to provide host authentication. This key-exchange method provides explicit server authentication. For more information about using DH key-exchange methods, see RFC 4253.

You must set the SSH key exchange in the Admin context; this setting is inherited by all other contexts.

Examples

The following example shows how to exchange keys using the DH Group 14 SHA1 key-exchange method:

```
ciscoasa(config)# ssh key-exchange group dh-group-14-sha1
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
crypto key generate rsa	Generates RSA key pairs for identity certificates.
debug ssh	Displays debugging information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh scopy enable	Enables a secure copy server on the ASA.
ssh version	Restricts the ASA to using either SSH Version 1 or SSH Version 2.

ssh key-exchange hostkey

If you do not want to use the default key order (EdDSA, ECDSA, and then RSA), identify the key pair you want to use wih the **ssh key-exchange hostkey** command in global configuration mode. To restore the default, use the **no** form of this command.

ssh key-exchange hostkey { **rsa** | **ecdsa** | **eddsa** }
no ssh key-exchange hostname

Syntax Description

ecdsa	Uses the ECDSA key only.
eddsa	Uses the EdDSA key only.
rsa	Uses the RSA key only. You must use a key size 2048 or higher. RSA key support will be removed in a later release, so we suggest using the other supported key types instead.

Command Default

By default, this command is disabled, and keys are tried in the following order: EdDSA, ECDSA, and then RSA.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes (Admin context only)	—

Command History

Release	Modification
9.16(1)	We introduced this command.

Usage Guidelines

SSH tries keys in the following order: EdDSA, ECDSA, and then RSA. View the keys using the **show crypto key mypubkey** {**eddsa** | **ecdsa** | **rsa**} command. The keys used by SSH are called <Default-*type*-Key>. If you override the key order with the **ssh key-exchange hostkey rsa** command,you must use a key size 2048 or higher. For upgrade compatibility, smaller keys are only supported when you use the default key order. RSA key support will be removed in a later release, so we suggest using the other supported key types instead.

Examples

The following example forces use of the EdDSA key only:

```
ciscoasa(config)# ssh key-exchange hostkey eddsa
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
crypto key generate rsa	Generates RSA key pairs for identity certificates.
debug ssh	Displays debugging information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh key-exchange group	Sets the SSH key exchange method.
ssh scopy enable	Enables a secure copy server on the ASA.

ssh pubkey-chain

To manually add or delete SSH servers and their keys from the ASA database for the on-board Secure Copy (SCP) client, use the **ssh pubkey-chain** command in global configuration mode. To remove all host keys, use the **no** form of this command. To remove only a single server key, see the **server** command.

ssh pubkey-chain
no ssh pubkey-chain

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.1(5)	This command was added.

Usage Guidelines

You can copy files to and from the ASA using the on-board SCP client. The ASA stores the SSH host key for each SCP server to which it connects. You can manually add or delete servers and their keys from the ASA database if desired.

For each server (see the **server** command), you can specify the **key-string** (public key) or **key-hash** (hashed value) of the SSH host.

Examples

The following example adds an already hashed host key for the server at 10.86.94.170:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

The following example adds a host string key for the server at 10.7.8.9:

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
```

```
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

Related Commands

Command	Description
copy	Copies a file to or from the ASA.
key-hash	Enters a hashed SSH host key.
key-string	Enters a public SSH host key.
server	Adds an SSH server and host key to the ASA database.
ssh stricthostkeycheck	Enables SSH host key checking for the on-board Secure Copy (SCP) client.

ssh scopy enable

To enable Secure Copy (SCP) on the ASA, use the **ssh scopy enable** command in global configuration mode. To disable SCP, use the **no** form of this command.

ssh scopy enable
no ssh scopy enable

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.1(7)/9.4(3)/9.5(3)/9.6(1)	You can configure encryption and integrity ciphers for SSH access using the **ssh cipher encryption** and **ssh cipher integrity** commands.

Usage Guidelines

SCP is a server-only implementation; it will be able to accept and terminate connections for SCP but can not initiate them. The ASA has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the ASA internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The ASA license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Before initiating the file transfer, the ASA checks available Flash memory. If there is not enough available space, the ASA terminates the SCP connection. If you are overwriting a file in Flash memory, you still need to have enough free space for the file being copied to the ASA. The SCP process copies the file to a temporary file first, then copies the temporary file over the file being replaced. If you do not have enough space in Flash to hold the file being copied and the file being overwritten, the ASA terminates the SCP connection.

The performance of secure copy depends partly on the encryption cipher used. By default, the ASA negotiates one of the following algorithms in order: 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr. If the first algorithm proposed (3des-cbc) is chosen, then the performance is much slower than a more efficient algorithm such as aes128-cbc. To change the proposed ciphers, use the **ssh cipher encryption** command; for example, **ssh cipher encryption custom aes128-cbc**.

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh scopy enable
ciscoasa(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the ASA from the specified client or network.
ssh version	Restricts the ASA to using either SSH Version 1 or SSH Version 2.

ssh stack ciscossh

To use the CiscoSSH stack, use the **ssh stack ciscossh** command in global configuration mode. To use the proprietary ASA SSH stack, use the **no** form of this command.

ssh stack ciscossh
no ssh stack ciscossh

Command Default

CiscoSSH stack is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.17(1)	This command was added.
9.19(1)	This command is now enabled by default.

Usage Guidelines

The ASA supports two SSH stacks for SSH connections: a proprietary SSH stack or the CiscoSSH stack. CiscoSSH is based on OpenSSH. Cisco SSH supports:

- FIPS compliance
- Regular updates, including updates from Cisco and the open source community

Note that the CiscoSSH stack does not support:

- SSH to a different interface over VPN (management-access)
- EdDSA key pair
- RSA key pair in FIPS mode

If you need these features, you should use the ASA SSH stack.

There is a small change to SCP functionality with the CiscoSSH stack: to use the ASA **copy** command to copy a file to or from an SCP server, you have to enable SSH access on the ASA for the SCP server subnet/host using the **ssh** command.

Examples

The following example shows how to disable the CiscoSSH stack.

```
ciscoasa(config)# no ssh stack ciscossh
ciscoasa(config)#
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the ASA from the specified client or network.

ssh stricthostkeycheck

To enable SSH host key checking for the on-board Secure Copy (SCP) client, use the **ssh stricthostkeycheck** command in global configuration mode. To disable host key checking, use the **no** form of this command.

ssh stricthostkeycheck
no ssh stricthostkeycheck

Syntax Description

This command has no arguments or keywords.

Command Default

By default, this command is enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.1(5)	This command was added.

Usage Guidelines

You can copy files to and from the ASA using the on-board SCP client. When this option is enabled, you are prompted to accept or reject the host key if it is not already stored on the ASA. When this option is disabled, the ASA accepts the host key automatically if it was not stored before.

Examples

The following example enables SSH host key checking:

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?
Address or name of remote host [10.86.95.9]?
Destination username [cisco]?
Destination password []? cisco123
Destination filename [x]?
```

Related Commands

Command	Description
copy	Copies a file to or from the ASA.

Command	Description
key-hash	Enters a hashed SSH host key.
key-string	Enters a public SSH host key.
server	Adds an SSH server and host key to the ASA database.
ssh pubkey-chain	Manually adds or deletes servers and their keys from the ASA database.

ssh timeout

To change the default SSH session idle timeout value, use the **ssh timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

ssh timeout *number*
no ssh timeout

Syntax Description

number	Specifies the duration in minutes that an SSH session can remain inactive before being disconnected. Valid values are from 1 to 60 minutes.

Command Default

The default session timeout value is 5 minutes.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ssh timeout command specifies the duration in minutes that a session can be idle before being disconnected. The default duration is 5 minutes.

Examples

The following example shows how to configure the inside interface to accept only SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.

Command	Description
show ssh sessions	Displays information about active SSH sessions to the ASA.
ssh disconnect	Disconnects an active SSH session.

ssh version (Deprecated)

To restrict the version of SSH accepted by the ASA, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command. Only Version 2 is supported.

ssh version 2
no ssh version 2

Syntax Description

2	Specifies that only SSH Version 2 connections are supported.

Command Default

Version 2 is the default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.9(1)	Version **1** was deprecated, and the **1** keyword will be removed in a later release. The default setting was also changed from **ssh version 1 2** to **ssh version 2** only.
9.16(1)	This command was removed.

Usage Guidelines

You should only set the SSH version to version 2.

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
ciscoasa(config)# ssh 10.1.1.1 255.255.255.0 inside
ciscoasa(config)# ssh version 2
ciscoasa(config)# ssh copy enable
ciscoasa(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.

Command	Description
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the ASA from the specified client or network.

ssl certificate-authentication

To enable client certificate authentication for backwards compatibility for versions previous to 8.2(1), use the **ssl certificate-authentication** command in global configuration mode. To disable ssl certificate authentication, use the **no** version of this command.

ssl certificate-authentication [**fca-timeout** *timeout-in minutes*] **interface** *interface-name* **port** *port-number*
no ssl certificate-authentication [**fca-timeout** *timeout-in minutes*] **interface** *interface-name* **port** *port-number*

Syntax Description

fca-timeout	Forced certificate authentication timeout value in minutes.
interface-name	The name of the selected interface, such as inside, management, and outside.
port-number	The TCP port number, an integer in the range 1-65535.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
8.0(3)	This command was added.
8.2(1)	This command is no longer needed, but the ASA retains it for downgrading to previous versions.

Usage Guidelines

This command replaces the deprecated **http authentication-certificate** command.

Examples

The following example shows how to configure the ASA to use the SSL certificate authentication feature:

```
ciscoasa
(config)#
 ssl certificate-authentication interface inside port 330
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured SSL commands.

ssl cipher

To specify the encryption algorithms for the SSL, DTLS, and TLS protocols, use the **ssl cipher** command in global configuration mode. To restore the default, which is the complete set of encryption algorithms, use the **no** form of this command.

ssl cipher *version* [*level* | **custom** *"string"*]
no ssl cipher *version* [*level* | **custom** *"string"*]

Syntax Description

custom *string*	Allows full control of the cipher suite using OpenSSL cipher definition strings.
level	Specifies the strength of the cipher and indicates the minimum level of ciphers that are supported. Valid values in increasing order of strength are: • **all**—Includes all ciphers, including NULL-SHA. • **low**—Includes all ciphers except NULL-SHA. • **medium**—Includes all ciphers except NULL-SHA, DES-CBC-SHA, and RC4-MD5. • **fips**—Includes all FIPS-compliant ciphers (excludes NULL-SHA, DES-CBC-SHA, RC4-MD5, RC4-SHA, and DES-CBC3-SHA. • **high** (applies only to TLSv1.2)—Includes only AES-256 with SHA-2 ciphers.
version	Specifies the SSL, DTLS, or TLS protocol version. Supported versions include: • **default**—The set of ciphers for outbound connections. • **dtlsv1**—The ciphers for DTLSv1 inbound connections. • dtlsv1.2 -The ciphers for DTLSv1.2 inbound connections. • **tlsv1**—The ciphers for TLSv1 inbound connections. • **tlsv1.1**—The ciphers for TLSv1.1 inbound connections. • **tlsv1.2**—The ciphers for TLSv1.2 inbound connections.

Command Default

The default is **medium** for all protocol versions.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.16(1)	Removed support for DES configuration on enabling strong crypto licensing because the DES is considered to be a weak cipher. If DES is configured when a strong licensing is enabled, DES is converted to strong cipher, AES.
9.12(1)	Removed NULL-SHA from tlv1 supported ciphers on lina. Deprecated and removed ssl cipher tlsv1 all and ssl cipher tlsv1 custom NULL-SHA command.
9.10(1)	dtls1.2 option added.
9.4(1)	All SSLv3 configuration and support removed from the ASA.
9.3(2)	This command was added.

Usage Guidelines

This command replaced the **ssl encryption** command starting with ASA Version 9.3(2).

The recommended setting is **medium**. Using **high** may limit connectivity. Using **custom** may limit functionality if there are only a few ciphers configured. Restricting the default custom value limits outbound connectivity, including clustering.

For more information about ciphers using OpenSSL, see https://www.openssl.org/docs/apps/ciphers.html.

Use the **show ssl ciphers all** command to view the list of which ciphers support which versions. For example:

```
These are the ciphers for the given cipher level; not all ciphers are supported by all
versions of SSL/TLS.
These names can be used to create a custom cipher list:
  DHE-RSA-AES256-SHA256 (tlsv1.2)
  AES256-SHA256 (tlsv1.2)
  DHE-RSA-AES128-SHA256 (tlsv1.2)
  AES128-SHA256 (tlsv1.2)
  DHE-RSA-AES256-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES256-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DHE-RSA-AES128-SHA (tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  AES128-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  DES-CBC3-SHA (sslv3, tlsv1, tlsv1.1, dtlsv1, tlsv1.2)
  RC4-SHA (sslv3, tlsv1)
  RC4-MD5 (sslv3, tlsv1)
  DES-CBC-SHA (sslv3, tlsv1)
  NULL-SHA (sslv3, tlsv1)
```

The ASA specifies the order of priority for supported ciphers as:

Ciphers supported by TLSv1.2 (1-9)

1. DHE-RSA-AES256-SHA256

2. AES256-SHA256
3. DHE-RSA-AES128-SHA256
4. AES128-SHA256
5. DHE-RSA-AES256-SHA
6. AES256-SHA
7. DHE-RSA-AES128-SHA
8. AES128-SHA
9. DES-CBC3-SHA

Ciphers not supported by TLSv1.1 or TLSv1.2 (10-13)

1. RC4-SHA
2. RC4-MD5
3. DES-CBC-SHA
4. NULL-SHA

Examples

The following example shows how to configure the ASA to use TLSv1.1 FIPS-compliant ciphers:

```
ciscoasa
(config)#

ssl cipher tlsv1.1 fips
```

The following example shows how to configure the ASA to use TLSv1 custom ciphers:

```
ciscoasa
(config)#
 ssl cipher tlsv1 custom "RC4-SHA:ALL"
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured SSL commands.
show ssl ciphers	Displays the list of supported ciphers.

ssl-client-certificate

To specify the certificate that the ASA should present to the LDAP server as the client certificate when using LDAPS, use the **ssl-client-certificate** command in aaa-server host configuration mode. To remove the certificate, use the **no** form of this command.

ssl-client-certificate *trustpoint_name*
no ssl-client-certificate *trustpoint_name*

Syntax Description

trustpoint_name	The name of the trustpoint that holds the certificate that the ASA should present to the LDAP server as the client certificate.

Command Default

No default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server host configuration (LDAP only)	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.18(1)	This command was added.

Usage Guidelines

This certificate is needed if you configure the LDAP server to verify the client certificate. You must also enable **ldap-over-ssl** for the server. If you do not configure a certificate, the ASA does not present one when the LDAP server asks for it. If an LDAP server is configured to require a peer certificate, the secure LDAP session will not complete and authentication/authorization requests will fail.

Example

The following example shows two LDAP servers using different trustpoints for client authentication.

```
asa(config)# show running-config aaa-server OPENLDAPS
aaa-server OPENLDAPS protocol ldap
aaa-server OPENLDAPS (manif) host 10.1.1.2
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn cn=admin,dc=example,dc=com
ldap-over-ssl enable
ssl-client-certificate LDAPS_TP_1
```

```
server-type auto-detect
aaa-server OPENLDAPS (manif) host 10.2.2.5
ldap-base-dn DC=example,DC=com
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn cn=admin,dc=example,dc=com
ldap-over-ssl enable
ssl-client-certificate LDAPS_TP_2
server-type auto-detect
```

Related Commands

Command	Description
ldap-over-ssl	Configures LDAPS as the communications protocol for the LDAP server.

ssl client-version

To specify the SSL/TLS protocol version that the ASA uses when acting as a client, use the **ssl client-version** command in global configuration mode. To revert to the default, use the **no** form of this command.

ssl client-version [**any** | **sslv3-only** | **tlsv1-only** | **sslv3** | **tlsv1** | **tlsv1.1** | **tlsv1.2**]
no ssl client-version

Syntax Description

any	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater).
sslv3	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater).
sslv3-only	Transmits SSLv3 client hellos and negotiates SSLv3 (or greater). **Note** This option has been deprecated as of Version 9.3(2).
tlsv1	Transmits TLSv1 client hellos and negotiates TLSv1 (or greater).
tlsv1.1	Transmits TLSv1.1 client hellos and negotiates TLSv1.1 (or greater).
tlsv1.2	Transmits TLSv1.2 client hellos and negotiates TLSv1.2 (or greater).
tlsv1-only	Transmits TLSv1 client hellos and negotiates TLSv1 (or greater). **Note** This option has been deprecated as of Version 9.3(2).

Command Default

The default value is **tlsv1**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	SSLv3 has been deprecated. The default is now **tlsv1** instead of **any**. The **any** keyword has been deprecated.

Usage Guidelines

If you use the **any**, **sslv3**, or **sslv3-only** keywords, the command is accepted with the following warning.

```
WARNING: SSLv3 is deprecated. Use of TLSv1 or greater is recommended.
```

In the next major ASA release, these keywords will be removed from the ASA.

Examples

The following example shows how to configure the ASA to specify the SSLv3 protocol version when acting as an SSL client:

```
ciscoasa
(config)#
 ssl client-version any
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
show running-config ssl	Displays the current set of configured SSL commands.
ssl server-version	Specifies the minimum protocol version for which the ASA will negotiate an SSL/TLS connection.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

ssl dh-group

To specify the Diffie-Hellmann (DH) group to be used with DHE-RSA ciphers that are used by TLS, use the **ssl dh-group** command in global configuration mode. To return to the default, use the **no** form of this command.

ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]
no ssl dh-group [**group1** | **group2** | **group5** | **group14** | **group24**]

Syntax Description

group1	Configures DH group 1 (768-bit modulus).
group2	Configures DH group 2 (1024-bit modulus).
group5	Configures DH group 5 (1536-bit modulus).
group14	Configures DH group 14 (2048-bit modulus, 224-bit prime order subgroup).
group24	Configures DH group 24 (2048-bit modulus, 256-bit prime order subgroup).

Command Default

The default is DH group 14.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.16(1)	Support is remove for the command options group2, group5, and group24. Support was added for the command option group15.
9.13(1)	The group2 and group 5 command option was deprecated and will be removed in the later release.
9.3(2)	This command was added.

Usage Guidelines

Groups 1 and 2 are compatible with Java 7 and earlier versions. Groups 5, 14, and 24 are not compatible with Java 7. All groups are compatible with Java 8. Groups 14 and 24 are FIPS-compliant.

Examples

The following example shows how to configure the ASA to use a specific DH group:

```
ciscoasa
(config)#
 ssl dh-group group14
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured SSL commands.

ssl ecdh-group

To specify the group to be used with ECDHE-ECDSA ciphers that are used by TLS, use the **ssl ecdh-group** command in global configuration mode. To return to the default, use the **no** form of this command.

ssl ecdh-group [**group19** | **group20** | **group21**]
no ssl ecdh-group [**group19** | **group20** | **group21**]

Syntax Description

group19	Configures group 19 (256-bit EC).
group20	Configures group 20 (384-bit EC).
group21	Configures group 21 (521-bit EC).

Command Default

The default is group 19.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
9.4(1)	This command was added.

Usage Guidelines

TLSv1.2 adds support for the following ciphers:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- RSA-AES128-GCM-SHA256

- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256

Note ECDSA and DHE ciphers are the highest priority.

Examples

The following example shows how to configure the ASA to use a specific DH group:

```
ciscoasa
(config)#
 ssl ecdh-group group21
```

Related Commands

Command	Description
show running-config ssl	Displays the current set of configured SSL commands.

ssl encryption (Deprecated)

Note The last supported release for this command was Version 9.3(1).

To specify the encryption algorithms for the SSL, DTLS, and TLS protocols, use the **ssl encryption** command in global configuration mode **.** To restore the default, which is the complete set of encryption algorithms, use the **no** form of this command.

ssl encryption [**3des-sha1**] [**aes128-sha1**] [**aes256-sha1**] [**des-sha1**] [**null-sha1**] [**rc4-md5**] [**rc4-sha1**] [**dhe-aes256-sha1**] [**dhe-aes128-sha1**]
no ssl encryption

Syntax Description

3des-sha1	Specifies triple DES 168-bit encryption with Secure Hash Algorithm 1 (FIPS-compliant).
aes128-sha1	Specifies triple AES 128-bit encryption with Secure Hash Algorithm 1 (FIPS-compliant).
aes256-sha1	Specifies triple AES 256-bit encryption with Secure Hash Algorithm 1 (FIPS-compliant).
dhe-aes128-sha1	Specifies AES 128-bit encryption cipher suites for Transport Layer Security (TLS) (FIPS-compliant).
dhe-aes256-sha1	Specifies AES 256-bit encryption cipher suites for Transport Layer Security (TLS) (FIPS-compliant).
des-sha1	Specifies DES 56-bit encryption with Secure Hash Algorithm 1.
null-sha1	Specifies null encryption with Secure Hash Algorithm 1. This setting enforces message integrity without confidentiality. **Caution** If you specify null-sha1, data is not encrypted.
rc4-md5	Specifies RC4 128-bit encryption with an MD5 hash function.
rc4-sha1	Specifies RC4 128-bit encryption with Secure Hash Algorithm 1.

Command Default

By default, the SSL encryption list on the ASA contains these algorithms in the following order:

1. RC4-SHA1
2. AES128-SHA1 (FIPS-compliant)
3. AES256-SHA1 (FIPS-compliant)
4. 3DES-SHA1 (FIPS-compliant)
5. DHE-AES256-SHA1 (FIPS-compliant)
6. DHE-AES128-SHA1 (FIPS-compliant)

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.1(2)	Support for SSL encryption using the DHE-AES128-SHA1 and DHE-AES256-SHA1 algorithms was added.
9.3(2)	This command was deprecated and has been replaced by the **ssl cipher** command.
9.12(1)	This command was removed.

Usage Guidelines

Issuing the command again overwrites the previous setting. The ASDM License tab reflects the maximum encryption that the license supports, not the value that you configure.

The ordering of the algorithms determines preference for their use. You can add or remove algorithms to meet the needs of your environment.

For FIPS-compliant Secure Client SSL connections, you must ensure a FIPS-compliant cipher is the first one specified in the list of SSL encryptions.

Several applications do not support DHE, so include at least one other SSL encryption method to ensure a cipher suite common to both.

Cryptographic operations use symmetric-key algorithms, as referenced in http://en.wikipedia.org/wiki/Symmetric-key_algorithm .

Examples

The following example shows how to configure the ASA to use the 3des-sha1 and des-sha1 encryption algorithms:

```
ciscoasa
(config)#
 ssl encryption 3des-sha1 des-sha1
```

Starting with ASA version 9.3(2)

The following examples show that this command has been deprecated and replaced by the **ssl cipher** command:

ciscoasa (config)# **ssl encryption ?**

```
configure mode commands/options:
This command is DEPRECATED, use 'ssl cipher' instead.
  3des-sha1        Indicate use of 3des-sha1 for ssl encryption
  aes128-sha1      Indicate use of aes128-sha1 for ssl encryption
  aes256-sha1      Indicate use of aes256-sha1 for ssl encryption
  des-sha1         Indicate use of des-sha1 for ssl encryption
  dhe-aes128-sha1  Indicate use of dhe-aes128-sha1 for ssl encryption
  dhe-aes256-sha1  Indicate use of dhe-aes256-sha1 for ssl encryption
  null-sha1        Indicate use of null-sha1 for ssl encryption (NOTE: Data is
                   NOT encrypted if this cipher is chosen)
  rc4-md5          Indicate use of rc4-md5 for ssl encryption
  rc4-sha1         Indicate use of rc4-sha1 for ssl encryption
```

ciscoasa (config)# **ssl encryption rc4-sha1 aes256-sha1 aes128-sha1**

```
WARNING: This command has been deprecated; use 'ssl cipher' instead.
INFO: Converting to: ssl cipher default custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher sslv3 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher tlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
INFO: Converting to: ssl cipher dtlsv1 custom "RC4-SHA:AES256-SHA:AES128-SHA"
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the ASA uses when acting as a client.
ssl server-version	Specifies the minimum protocol version for which the ASA will negotiate an SSL/TLS connection.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.
ssl cipher	Specifies the encryption algorithms for the SSL, DTLS, and TLS protocols. **Note** Available as of the 9.3(2) release.

ssl server-version

To set the minimum protocol version for which the ASA will negotiate an SSL/TLS connection, use the **ssl server-version** command in global configuration mode. To revert to the default, any, use the **no** form of this command.

ssl server-version [[**tlsv1 | tlsv1.1 | tlsv1.2**] [**dtlsv1 | dtlsv1.2**]]
no ssl server-version

Syntax Description

tlsv1	Accepts SSLv2 client hellos and negotiates TLSv1 (or greater).
tlsv1.1	Accepts SSLv2 client hellos and negotiates TLSv1.1 (or greater).
tlsv1.2	Accepts SSLv2 client hellos and negotiates TLSv1.2 (or greater).
dtlsv1	Accepts DTLSv1 client hellos and negotiates DTLSv1 (or greater).
dtlsvv1.2	Accepts DTLSv1.2 client hellos and negotiates DTLSv1.2 (or greater). Specifying DTLSv1.2 tunnel use requires the specification of TLSv1.2 tunnel since it is the only valid option.

Command Default

The default values are **tlsv1** and **dtlsv1** .

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	SSLv3 has been deprecated. The default is now **tlsv1** instead of **any** . The **any** keyword has been deprecated.
9.4(1)	All SSLv3 keywords have been removed from the ASA configuration, and SSLv3 support has been removed from the ASA. If you have SSLv3 enabled, a boot-time error will appear from the command with the SSLv3 option. The ASA will then revert to the default use of TLSv1.
9.10(1)	DTLS options provided now that DTLSv1.2 is supported.Previously assumed DTLS version 1 remains the default.

Examples

The following example shows how to configure the ASA to negotiate an SSL/TLS connection:

```
ciscoasa
(config)#
 ssl server-version tlsv1
```

The following example shows configuration and verification of set versions:

```
ciscoasa (config)# ssl server-version tlsv1.2 dtlsv1.2

ciscoasa (config)# sh run ssl
ssl server-version tlsv1.2 dtlsv1.2
ciscoasa (config)# no ssl server-version
ciscoasa (config)# sh run all ssl
ssl server-version tlsv1 dtlsv1
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version that the ASA uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.

ssl trust-point

To specify the certificate trustpoint that represents the SSL certificate for an interface, use the **ssl trust-point** command with the *interface* argument in global configuration mode. To remove an SSL trustpoint from the configuration that does not specify an interface, use the **no** form of this command. To remove an entry that does specify an interface, use the no **ssl trust-point** *name* [*interface*] form of the command.

ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]
no ssl trust-point *name* [*interface* [**vpnlb-ip**] | **domain** *domain-name*]

Syntax Description

domain *domain-name*	Associates this trustpoint with a particular domain name that is used to access this interface (for example, www.cisco.com).
interface	Specifies the name for the interface to which the trustpoint applies. The **nameif** command defines the name of the interface.
name	Specifies the name of the CA trustpoint as configured in the **crypto ca trustpoint** *name* command.
vpnlb-ip	Associates this trustpoint with the VPN load-balancing cluster IP address on this interface. Applies only to interfaces.

Command Default

The default is no trustpoint association. The ASA uses the default self-generated RSA key-pair certificate.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.
9.3(2)	The **domain** *domain-name* keyword-argument pair was added.

Usage Guidelines

If you do not specify an interface or domain, then this entry will represent the fallback trustpoint that is used on all interfaces that are not associated with a trustpoint of their own.

If you enter the **ssl trustpoint ?** command, the available configured trustpoints appear. If you enter the **ssl trust-point** *name* **?** command (for example, **ssl trust-point mysslcert ?**), the available configured interfaces for the trustpoint-SSL certificate association appear.

You may configure up to 16 trustpoints per interface.

Observe these guidelines when using this command:

- The value for *trustpoint* must be the name of the CA trustpoint as configured in the **crypto ca trustpoint** *name* command.
- The value for *interface* must be the *nameif* name of a previously configured interface.
- Removing a trustpoint also removes any **ssl trust-point** entries that reference that trustpoint.
- You can have one **ssl trust-point** entry for each interface and one that specifies no interfaces.
- A trustpoint configured with the **domain** keyword may apply to multiple interfaces (depending on how you connect).
- You may only have one **ssl trust-point** per *domain-name* value.
- You can reuse the same trustpoint for multiple entries.
- If the following error appears after you enter this command:

```
error:0B080074:x509 certificate routines:X509_check_private_key:key values
mismatch@x509_cmp.c:339
```

It means that a user has configured a new certificate to replace a previously configured certificate. No action is required.

- The certificates are chosen in the following order:
  - If a connection matches the value of the **domain** keyword, that certificate is chosen first. (**ssl trust-point** *name* **domain** *domain-name* command)
  - If a connection is made to the load-balancing address, the vpnlb-ip certificate is chosen. (**ssl trust-point** *name* **interface** **vpnlb-ip** command)
  - The certificate configured for the interface. (**ssl trust-point** *name* **interface** command)
  - The default certificate not associated with an interface. (**ssl trust-point** *name* command)
  - The ASA's self-signed, self-generated certificate.

Examples

The following example shows how to configure an SSL trustpoint called FirstTrust for the inside interface, and a trustpoint called DefaultTrust with no associated interface.

```
ciscoasa
(config)#
 ssl trust-point FirstTrust inside
ciscoasa
(config)#
 ssl trust-point DefaultTrust
```

The following example shows how to use the **no** form of the command to delete a trustpoint that has no associated interface:

```
ciscoasa
(config)#
 show running-configuration ssl
```

```
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa(config)# no ssl trust-point
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point FirstTrust inside
```

The following example shows how to delete a trustpoint that does have an associated interface:

```
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
ciscoasa
(config)#
 no ssl trust-point FirstTrust inside
ciscoasa
(config)#
 show running-configuration ssl
ssl trust-point DefaultTrust
```

The following example shows how to assign a specific domain name to a configured trustpoint:

```
ciscoasa
(config)#
 ssl trust-point
           www-cert domain www.example.com
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the ASA uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl server-version	Specifies the minimum protocol version for which the ASA will negotiate an SSL/TLS connection.
show ssl	Displays SSL configuration statistics.

sso-server (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To create a Single Sign-On (SSO) server for ASA user authentication, use the **sso-server** command in webvpn configuration mode. With this command, you must specify the SSO server type.

To remove an SSO server, use the **no** form of this command.

sso-server *name* **type** [*siteminder* | *saml-v1.1-post*]
no sso-server *name*

Note This command is required for SSO authentication.

Syntax Description

name	Specifies the name of the SSO server. Minimum of 4 characters and maximum of 31 characters.
saml-v1.1-post	Specifies that the ASA SSO server being configured is a SAML, Version 1.1, SSO server of the POST type.
siteminder	Specifies that the ASA SSO server being configured is a Computer Associates SiteMinder SSO server.
type	Specifies the type of SSO server. SiteMinder and SAML-V1.1-POST are the only types available.

Command Default

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The **sso-server** command lets you create an SSO server.

In the authentication, the ASA acts as a proxy for the WebVPN user to the SSO server. The ASA currently supports the SiteMinder SSO server (formerly Netegrity SiteMinder) and the SAML POST-type SSO server. Currently, the available arguments for the type option are restricted to *siteminder* or *saml-V1.1-post* .

Examples

The following example, entered in webvpn configuration mode, creates a SiteMinder-type SSO server named “example1”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example1 type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
```

The following example, entered in webvpn configuration mode, creates a SAML, Version 1.1, POST-type SSO server named “example2”:

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# sso-server example2 type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml)#
```

Related Commands

Command	Description
assertion-consumer-url	Identifies the URL for the SAML-type SSO assertion consumer service.
issuer	Specifies the SAML-type SSO server’s security device name.
max-retry-attempts	Configures the number of times the ASA retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for an SSO server.
test sso-server	Tests an SSO server with a trial authentication request.
trustpoint	Specifies a trustpoint name that contains the certificate to use to sign the SAML-type browser assertion
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

sso-server value (group-policy webvpn) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To assign an SSO server to a group policy, use the **sso-server value** command in webvpn configuration mode available in group-policy configuration mode.

To remove the assignment and use the default policy, use the **no** form of this command.

To prevent inheriting the default policy, use the **sso-server none** command.

sso-server { **value** *name* | **none** }
[**no**] **sso-server value** *name*

Syntax Description

name	Specifies the name of the SSO server being assigned to the group policy.

Command Default

The default policy assigned to the group is DfltGrpPolicy.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

The **sso-server value** command, when entered in group-policy webvpn mode, lets you assign an SSO server to a group policy.

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

Note Enter the same command, **sso-server value** , in username-webvpn configuration mode to assign SSO servers to user policies.

Examples

The following example commands create the group policy my-sso-grp-pol and assigns it to the SSO server named example:

```
ciscoasa(config)# group-policy my-sso-grp-pol internal
ciscoasa(config)# group-policy my-sso-grp-pol attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# sso-server value example
ciscoasa(config-group-webvpn)#
```

Related Commands

Command	Description
policy-server-secre t	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
sso-server value (username webvpn)	Assigns an SSO server to a user policy.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder-type SSO authentication requests.

sso-server value (username webvpn) (Deprecated)

Note The last supported release for this command was Version 9.5(1).

To assign an SSO server to a user policy, use the **sso-server value** command in webvpn configuration mode available in username configuration mode.

To remove an SSO server assignment for a user, use the **no** form of this command.

When a user policy inherits an unwanted SSO server assignment from a group policy, use the **sso-server none** command to remove the assignment.

sso-server { **value** *name* | **none** }
[**no**] **sso-server value** *name*

Syntax Description

name	Specifies the name of the SSO server being assigned to the user policy.

Command Default

The default is for the user policy to use the SSO server assignment in the group policy.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Username webvpn configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.
9.5(2)	This command was deprecated due to support for SAML 2.0.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without entering a username and password more than once. The ASA currently supports the SiteMinder-type of SSO server and the SAML POST-type SSO server.

This command applies to both types of SSO Servers.

The **sso-server value** command lets you assign an SSO server to a user policy.

Note Enter the same command, **sso-server value**, in group-webvpn configuration mode to assign SSO servers to group policies.

Examples

The following example commands assign the SSO server named my-sso-server to the user policy for a WebVPN user named Anyuser:

```
ciscoasa(config)# username Anyuser attributes
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# sso-server value my-sso-server
ciscoasa(config-username-webvpn)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to a SiteMinder SSO server.
show webvpn sso-server	Displays the operating statistics for all SSO servers configured on the security device.
sso-server	Creates a single sign-on server.
sso-server value (config-group-webvpn)	Assigns an SSO server to a group policy.
web-agent-url	Specifies the SSO server URL to which the ASA makes SiteMinder SSO authentication requests.

start-port

To configure the starting port for the port pool in the basic mapping rule in a Mapping Address and Port (MAP) domain, use the **start-port** command in MAP domain basic mapping rule configuration mode. Use the **no** form of this command to remove the ratio.

start-port*number*
no start-port *number*

Syntax Description

number	The first port in the port pool for the translated address. The port you specify must be a power of 2, from 1-32768 such as 1, 2, 4, 8, and so forth. If you want to exclude the well-known ports, start at 1024 or higher.

Command Default

No defaults.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MAP domain basic mapping rule configuration mode.	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.13(1)	This command was introduced.

Usage Guidelines

The **start-port** and **share-ratio** commands in the basic mapping rule determine the starting port and number of ports in the pool used to translate addresses within a MAP domain.

Examples

The following example creates a MAP-T domain named 1 and configures the translation rules for the domain.

```
ciscoasa(config)# map-domain 1

ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64

ciscoasa(config-map-domain)# basic-mapping-rule

ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0

ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024

ciscoasa(config-map-domain-bmr)# share-ratio 16
```

Related Commands

Commands	Description
basic-mapping-rule	Configures the basic mapping rule for a MAP domain.
default-mapping-rule	Configures the default mapping rule for a MAP domain.
ipv4-prefix	Configures the IPv4 prefix for the basic mapping rule in a MAP domain.
ipv6-prefix	Configures the IPv6 prefix for the basic mapping rule in a MAP domain.
map-domain	Configures a Mapping Address and Port (MAP) domain.
share-ratio	Configures the number of ports in the basic mapping rule in a MAP domain.
show map-domain	Displays information about Mapping Address and Port (MAP) domains.
start-port	Configures the starting port for the basic mapping rule in a MAP domain.

start-url

To enter the URL at which to retrieve an optional pre-login cookie, use the **start-url** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command.

start-url *string*

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The URL for an SSO server. The maximum URL length is 1024 characters.

Command Default

There is no default value or behavior.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server-host configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

The WebVPN server of the ASA can use an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The authenticating web server may execute a pre-login sequence by sending a Set-Cookie header along with the login page content. You can discover this by connecting directly to the authenticating web server's login page with your browser. If the web server sets a cookie when the login page loads and if this cookie is relevant for the following login session, you must use the **start-url** command to enter the URL at which the cookie is retrieved. The actual login sequence starts after the pre-login cookie sequence with the form submission to the authenticating web server.

Note The **start-url** command is only required in the presence of the pre-login cookie exchange.

Examples

The following example, entered in aaa-server host configuration mode, specifies a URL for retrieving the pre-login cookie of https://example.com/east/Area.do?Page-Grp1:

```
ciscoasa(config)# aaa-server testgrp1 (inside) host example.com
ciscoasa(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
ciscoasa(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

state-checking

To enforce state checking for H.323, use the **state-checking** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

state-checking [**h225** | **ras**]
no state-checking [**h225** | **ras**]

Syntax Description

h225	Enforces state checking for H.225.
ras	Enforces state checking for RAS.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enforce state checking for RAS on an H.323 call:

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# state-checking ras
```

Related Commands

Command	Description
policy-map type inspect	Creates an inspection policy map.
show running-config policy-map	Display all current policy map configurations.

storage-url

To allow each context to use flash memory to store VPN packages, use the **storage-url** command in context configuration mode. To remove the storage space, use the **no** form of this command.

storage-url { **private | shared** } [**disk** *n* **:** /] *path* [*context_label*]
no storage-url { **private | shared** } [**disk** *n* **:** /] *path* [*context_label*]

Syntax Description

private	Assigns a private storage space to the context. You can specify one private storage space per context.
shared	Assigns a shared storage space to the context. You can specify one read-only shared storage space per context, but you can create multiple shared directories.
[**disk***n***:**/]*path*	Sets the path to the storage space. If you do not specify the disk number, the default is **disk0**. Under the specified path for the private storage space, the ASA creates a sub-directory named after the context. For example, for contextA if you specify **disk1:/private-storage** for the path, then the ASA creates a sub-directory for this context at disk1:/private-storage/contextA/. The ASA does not create context sub-directories for the shared storage space because it is a shared space for multiple contexts.
context_label	(Optional) You can name the path within the context with a *context_label* , so that the file system is not exposed to context administrators. For example, if you specify the *context_label* as **context**, then from within the context, this directory is called **context:**.

Command Default

If you do not specify the disk number, the default is **disk0**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Context configuration	• Yes	• Yes	—	—	• Yes

Command History

Release	Modification
9.6(2)	We introduced this command.

Usage Guidelines

Allow each context to use flash memory to store VPN packages, such as Secure Client, as well as providing storage for Secure Client and clientless SSL VPN portal customizations. Each context can use a private storage space as well as a shared read-only storage space. Note: Make sure the target directory is already present on the specified disk using the **mkdir** command.

You can specify one private storage space per context. You can read/write/delete from this directory within the context (as well as from the system execution space). To control how much disk space is allowed per context, see the **limit-resource storage** command.

To reduce duplication of common large files that can be ASA among all contexts, such as Secure Client packages, you can use the shared storage space. Only the system execution space can write and delete from the shared directory.

Examples

The following example creates a private directory and a shared directory, and assigns them to the admin context:

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

Related Commands

Command	Description
limit-resource storage	Controls how much disk space is allowed per context.

storage-key

To specify a storage key to protect the date stored between sessions, use the **storage-key** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

storage-key { **none** | **value** *string* }
nostorage-key

Syntax Description

string	Specifies a string to use as the value of the storage key. This string can be up to 64 characters long.

Command Default

The default is **none**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

While you can use any character except spaces in the storage key value, we recommend using only the standard alphanumeric character set: 0 through 9 and a through z.

Examples

The following example sets the storage key to the value abc123:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
storage-key value abc123
```

Related Commands

Command	Description
storage-objects	Configures storage objects for the data stored between sessions.

storage-objects

To specify which storage objects to use for the data stored between sessions, use the **storage-objects** command in group-policy webvpn configuration mode. To remove this command from the configuration, use the **no** version of this command.

storage-objects { **none | value** *string* }
no storage-objects

Syntax Description

string	Specifies the name of the storage objects. This string can be up to 64 characters long.

Command Default

The default is **none**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Group-policy webvpn configuration mode	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

While you can use any character except spaces and commas in the storage object name, we recommend using only the standard alphanumeric character set: 0 through 9 and a through z. Use a comma, with no space, to separate the names of storage objects in the string.

Examples

The following example sets the storage object names to cookies and xyz456:

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
storage-object value cookies,xyz456
```

Related Commands

Command	Description
storage-key	Configures storage key to use for the data stored between sessions.
user-storage	Configures a location for storing user data between sessions

strict-asp-state

To enable strict M3UA application server process (ASP) state validation, use the **strict-asp-state** command in policy map parameters configuration mode. Use the **no** form of this command to remove the setting.

strict-asp-state
no strict-asp-state

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.7(1)	This command was introduced.

Usage Guidelines

Use this command when configuring an M3UA inspection policy map.

If you enable strict application server process (ASP) state validation, the system maintains the ASP states of M3UA sessions and allows or drops ASP messages based on the validation result. If you do not enable strict ASP state validation, all ASP messages are forwarded uninspected.

Strict ASP state checking is required if you want stateful failover or if you want to operate within a cluster. However, strict ASP state checking works in Override mode only, it does not work if you are running in Loadsharing or Broadcast mode (per RFC 4666). The inspection assumes there is one and only one ASP per endpoint.

Examples

The following example enables strict checking for states and sessions:

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# strict-asp-state
```

Related Commands

Commands	Description
inspect m3ua	Enables M3UA inspection.

Commands	Description
policy-map type inspect m3ua	Creates an M3UA inspection policy map.

strict-diameter

To enable strict Diameter protocol conformance to RFC 6733, use the **strict-diameter** command in policy map parameters configuration mode. Use the **no** form of this command to remove the setting.

strict-diameter { **state** | **session** }
no strict-diameter { **state** | **session** }

Syntax Description

state	Enable state machine validation.
session	Enable session-related message validation.

Command Default

By default, inspection ensures that Diameter frames comply with the RFC, but state and session checking are not enabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	This command was introduced.

Usage Guidelines

Use this command when configuring a Diameter inspection policy map.

These options enable strict compliance validation for states and sessions in addition to standard protocol conformance checks. You can enter the command twice to enable both state and session checking.

Examples

The following example enables strict checking for states and sessions:

```
ciscoasa(config)# policy-map type inspect diameter diameter-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# strict-diameter state
ciscoasa(config-pmap-p)# strict-diameter session
```

Related Commands

Commands	Description
inspect diameter	Enables Diameter inspection.

Commands	Description
policy-map type inspect diameter	Creates a Diameter inspection policy map.

strict-header-validation

To enable strict validation of the header fields in the SIP messages according to RFC 3261, use the **strict-header-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

strict-header-validation action { **drop | drop-connection | reset | log** } { **log** }
no strict-header-validation action { **drop | drop-connection | reset | log** } { **log** }

Syntax Description

drop	Drops the packet if validation occurs.
drop-connection	Drops the connection of a violation occurs.
reset	Resets the connection of a violation occurs.
log	Specifies standalone or additional log in case of violation. It can be associated to any of the actions.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Parameters configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following example shows how to enable strict validation of SIP header fields in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# strict-header-validation action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

strict-http

To allow forwarding of non-compliant HTTP traffic, use the **strict-http** command in HTTP map configuration mode, which is accessible using the **http-map** command. To reset this feature to its default behavior, use the **no** form of the command.

strict-http action { **allow** | **reset** | **drop** } [**log**]
no strict-http action action { **allow** | **reset** | **drop** } [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generate a syslog.
reset	Closes the connection with a TCP reset message to client and server.

Command Default

This command is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
HTTP map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the ASA to allow forwarding of non-compliant HTTP traffic. This command overrides the default behavior, which is to deny forwarding of non-compliant HTTP traffic.

Examples

The following example allows forwarding of non-compliant HTTP traffic:

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# strict-http allow
ciscoasa(config-http-map)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

strip-group

This command applies only to usernames received in the form user@realm. A realm is an administrative domain appended to a username with the "@" delimiter (juser@abc).

To enable or disable strip-group processing, use the **strip-group** command in tunnel-group general-attributes mode. The ASA selects the tunnel group for IPsec connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the ASA sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the ASA sends the entire username including the realm.

To disable strip-group processing, use the **no** form of this command.

strip-group
no strip-group

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

You can apply this attribute only to the IPsec remote access tunnel-type.

Note Because of a limitation of MSCHAPv2, you cannot perform tunnel group switching when MSCHAPv2 is used for PPP authentication. The hash computation during MSCHAPv2 is bound to the username string (such as user + delimit + group).

Examples

The following example configures a remote access tunnel group named "remotegrp" for type IPsec remote access, then enters general configuration mode, sets the tunnel group named "remotegrp" as the default group policy, and then enables strip group for that tunnel group:

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-group
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

strip-realm

To enable or disable strip-realm processing, use the **strip-realm** command in tunnel-group general-attributes configuration mode. Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. A realm is an administrative domain appended to a username with the @ delimiter (username@realm). If the command is enabled, the ASA sends only the user part of the username authorization/authentication. Otherwise, the ASA sends the entire username.

To disable strip-realm processing, use the **no** form of this command.

strip-realm
no strip-realm

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting for this command is disabled.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group general attributes configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.0.1	This command was added.

Usage Guidelines

You can apply this attribute only to the IPsec remote access tunnel-type.

Examples

The following example configures a remote access tunnel group named “remotegrp” for type IPsec remote access, then enters general configuration mode, sets the tunnel group named “remotegrp” as the default group policy, and then enables strip realm for that tunnel group:

```
ciscoasa(config)# tunnel-group remotegrp type IPsec_ra
ciscoasa(config)# tunnel-group remotegrp general
ciscoasa(config-tunnel-general)# default-group-policy remotegrp
ciscoasa(config-tunnel-general)# strip-real
```

su – sz

subject-name (crypto ca certificate map)

To indicate that rule entry is applied to the subject DN of the IPsec peer certificate, use the **subject-name** command in crypto ca certificate map configuration mode. To remove an subject-name, use the **no** form of the command.

subject-name [**attr** *tag* **eq | ne | co | nc** *string*]
no subject-name [**attr** *tag* **eq | ne | co | nc** *string*]

Syntax Description

attr *tag*	Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows: DNQ = DN qualifierGENQ = Generational qualifierI = InitialsGN = Given nameN = NameSN = SurnameIP = IP addressSER = Serial numberUNAME = Unstructured nameEA = Email addressT = TitleO = Organization NameL = LocalitySP = State/ProvinceC = CountryOU = Organizational unitCN = Common name
co	Specifies that the rule entry string must be a substring in the DN string or indicated attribute.
eq	Specifies that the DN string or indicated attribute must match the entire rule string.
nc	Specifies that the rule entry string must not be a substring in theDN string or indicated attribute.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
string	Specifies the value to be matched.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca certificate map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters the ca certificate map configuration mode for certificate map 1 and creates a rule entry indicating that the Organization attribute of the certificate subject name must be equal to Central:

```
ciscoasa(config)# crypto ca certificate map 1
ciscoasa(ca-certificate-map)# subject-name attr o eq central
ciscoasa(ca-certificate-map)# exit
```

Related Commands

Command	Description
crypto ca certificate map	Enters ca certificate map configuration mode.
issuer-name	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

subject-name (crypto ca trustpoint)

To include the indicated subject DN in the certificate during enrollment, use the **subject-name** command in crypto ca trustpoint configuration mode. This is the person or system that uses the certificate. To restore the default setting, use the **no** form of the command.

subject-name *X.500_name*
no subject-name

Syntax Description

X.500_name	Defines the X.500 distinguished name. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains commas or spaces. For example: **cn=crl,ou=certs,o="cisco systems, inc.",c=US** . The maximum length is 500 characters.

Command Default

The default setting is not to include the subject name.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.0(1)	This command was added.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and sets up automatic enrollment at the URL https//:frog.example.com and includes the subject DN OU certs in the enrollment request for trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url http://frog.example.com/
ciscoasa(ca-trustpoint)# subject-name ou=certs
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment url	Specifies the URL for enrolling with a CA.

subject-name-default

To specify a generic subject-name distinguished name (DN) to be appended to the username in all user certificates issued by the local CA server, use the **subject-name-default** command in CA server configuration mode. To reset the subject-name DN to the default value, use the **no** form of this command.

subject-name-default *dn*
no subject-name-default

Syntax Description

dn	Specifies the generic subject-name DN included with a username in all user certificates issued by the local CA server. Supported DN attributes are cn (common name), ou (organizational unit), ol (organization locality), st (state), ea (e-mail address), c (company), t (title), and sn (surname). Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. The *dn* can be up to 500 characters.

Command Default

This command is not part of the default configuration. This command specifies the default DN in the certificate. The ASA ignores this command if the user entry has a DN.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
CA server configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The **subject-name-default** command specifies a common, generic DN to be used with a username to form a subject name for issued certificates. The *dn* value cn=username is sufficient for this purpose. This command eliminates the need to define a subject-name DN specifically for each user. The DN field is optional when a user is added using the **crypto ca server user-db add** dn *dn* command.

The ASA uses this command only when issuing certificates if a user entry does not specify a DN.

Examples

The following example specifies a DN:

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma, c="cisco systems, inc.”
ciscoasa
```

```
(config-ca-server)
#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
keysize	Specifies the size of the public and private keys generated at user certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate, issued certificates, or the CRL.

subnet

To configure a network for a network or network-service object, use the **subnet** command in object configuration mode. Use the **no** form of this command to remove the object from the configuration.

subnet { *IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix* } [*service*]
no subnet { *IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix* } [*service*]

Syntax Description

IPv4_address IPv4_mask	Specifies the IPv4 network address and subnet mask, separated by a space.
IPv6_address/IPv6_prefix	Specifies the IPv6 network address and prefix length, separated by a / character, no spaces.
service	(Optional; network-service object only.) Specify the service only if you want to limit the scope of the connections matched. By default, any connection to the resolved IP addresses matches the object. *protocol* [*operator port*] where: • *protocol* is the protocol used in the connection, such as tcp, udp, ip, and so forth. Use ? to see the list of protocols. • (TCP/UDP only.) *operator* is one of the following: • **eq** equals the port number specified. • **lt** means any port less than the specified port number. • **gt** means any port greater than the specified port number. • **range** means any port between the two ports specified. • (TCP/UDP only.) *port* is the port number, 1-65535 or a mnemonic, such as www. Use ? to see the mnemonics. For ranges, you must specify two ports, with the first port being a lower number than the second port.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network or network-service configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.3(1)	This command was added.
9.17(1)	Support for network-service objects, and the *service* keywords, were added.

Usage Guidelines

If you configure an existing object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a subnet network object:

```
ciscoasa(config)# object network OBJECT_SUBNET
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
```

The following example shows how to create a subnet network-service object for HTTPS traffic:

```
ciscoasa(config)# object network-service partner-web
ciscoasa(config-ns)# subnet 10.100.10.0 255.255.255.0 tcp eq 443
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.
fqdn	Specifies a fully-qualified domain name network object.
host	Specifies a host network object.
nat	Enables NAT for the network object.
object network	Creates a network object.
object network-service	Creates a network-service object.
object-group network	Creates a network object group.
object-group network-service	Creates a network-service object group.
range	Specifies a range of addresses for the network object.
show running-config object network	Shows the network object configuration.

summary-address (interface)

To configure a summary for EIGRP on a specific interface, use the **summary-address** command in interface configuration mode. To remove the summary address, use the **no** form of this command.

summary-address *as-number addr mask* [*admin-distance*]
no summary-address *as-number addr mask*

Syntax Description

as-number	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.
addr	The summary IP address.
mask	The subnet mask to apply to the IP address.
admin-distance	(Optional) The administrative distance of the summary route. Valid values are from 0 to 255. If not specified, the default value is 5.

Command Default

The defaults are as follows:

- EIGRP automatically summarizes routes to the network level, even for a single host route.
- The administrative distance of EIGRP summary routes is 5.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

By default, EIGRP summarizes subnet routes to the network level. Use the **no auto-summary** command to disable automatic route summarization. Using the **summary-address** command lets you manually define subnet route summaries on a per-interface basis.

Examples

The following example configures route summarization with a **tag** set to 3:

```
ciscoasa(config-if)# summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
ciscoasa(config-if)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

The following example removes the **summary-address** command from the configuration:

```
ciscoasa(config-if)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-if)#
```

Related Commands

Command	Description
auto-summary	Automatically creates summary addresses for the EIGRP routing process.

summary-prefix (ipv6 router ospf)

To configure an IPv6 summary prefix, use the **summary-prefix** command in ipv6 router ospf configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]
no summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

not-advertise	(Optional) Suppresses routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only.
prefix	Specifies the IPv6 prefix for the destination.
tag *tag_value*	(Optional) Specifies the tag value that can be used as a match value for controlling redistribution by means of route maps. This keyword applies to OSPFv3 only.

Command Default

The defaults are as follows:

- *tag_value* is 0.
- Routes that match the specified prefix and mask pair are not suppressed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
IPv6 router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.0(1)	This command was added.

Usage Guidelines

Use this command to configure an IPv6 summary prefix.

Examples

In the following example, the summary prefix FECO::/24 includes addresses FECO::/1 through FECO::/24. Only the address FECO::/24 is advertised in an external LSA:

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 172.16.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
redistribute	Redistributes IPv6 routes from one OSPFv3 routing domain into another OSPFv3 routing domain.

summary-address (router isis)

To create aggregate addresses for IS-IS, use the **summary-address** command in router isis configuration mode. To restore the default values, use the **no** form of this command.

summary-address *address mask* [**level-1 | level-1-2 | level-2**] [**tag** *tag-number*] [**metric** *metric-value*]
no summary-address *address mask* [**level-1 | level-1-2 | level-2**] [**tag** *tag-number*] [**metric** *metric-value*]

Syntax Description

level-1	(Optional) Only routes redistributed into Level 1 are summarized with the configured address and mask value.
level-1-2	(Optional) Summary routes are applied when redistributing routes into Level 1 and Level 2 IS-IS, and when Level 2 IS-IS advertises Level 1 routes as reachable in its area.
level-2	(Optional) Routes learned by Level 1 routing are summarized into the Level 2 backbone with the configured address and mask value. Redistributed routes into Level 2 IS-IS will be summarized also.
address	Summary address designated for a range of addresses.
mask	IP subnet mask used for the summary route.
tag *tag-number*	(Optional) Specifies the integer used to tag the summary route.
metric *metric-value*	(Optional) Specifies the metric value applied to the summary route.

Command Default

All routes are advertised individually.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router isis configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.6(1)	We introduced this command.

Usage Guidelines

Multiple groups of addresses can be summarized for a given level. Routes learned from other routing protocols can also be summarized. The metric used to advertise the summary is the smallest metric of all the more specific routes. This command helps reduce the size of the routing table.

This command also reduces the size of the link-state packets (LSPs) and thus the link-state database (LSDB). It also helps network stability because a summary advertisement is depending on many more specific routes. A single route flap does not cause the summary advertisement to flap in most cases.

The drawback of summary addresses is that other routes might have less information to calculate the most optimal routing table for all individual destinations.

Examples

The following example redistributes Routing Information Protocol (RIP) routes into IS-IS. In a RIP network, there are IP routes for 10.1.1, 10.1.2, 10.1.3, 10.1.4, and so on. This example advertises only 10.1.0.0 into the IS-IS Level 1 link-state protocol data unit (PDU). The summary address is tagged with 100 and given a metric value of 110.

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 01.0000.0000.0001.00
ciscoasa(config-router)# redistribute rip level-1 metric 40
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

Related Commands

Command	Description
advertise passive-only	Configures the ASA to advertise passive interfaces.
area-password	Configures an IS-IS area authentication password.
authentication key	Enables authentication for IS-IS globally.
authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance globally.
authentication send-only	Configure the IS-IS instance globally to have authentication performed only on IS-IS packets being sent (not received).
clear isis	Clears IS-IS data structures.
default-information originate	Generates a default route into an IS-IS routing domain.
distance	Defines the administrative distance assigned to routes discovered by the IS-IS protocol.
domain-password	Configures an IS-IS domain authentication password.
fast-flood	Configures IS-IS LSPs to be full.
hello padding	Configures IS-IS hellos to the full MTU size.
hostname dynamic	Enables IS-IS dynamic hostname capability.
ignore-lsp-errors	Configures the ASA to ignore IS-IS LSPs that are received with internal checksum errors rather than purging the LSPs.
isis adjacency-filter	Filters the establishment of IS-IS adjacencies.
isis advertise-prefix	Advertises IS-IS prefixes of connected networks in LSP advertisements on an IS-IS interface.

Command	Description
isis authentication key	Enables authentication for an interface.
isis authentication mode	Specifies the type of authentication mode used in IS-IS packets for the IS-IS instance per interface
isis authentication send-only	Configure the IS-IS instance per interface to have authentication performed only on IS-IS packets being sent (not received).
isis circuit-type	Configures the type of adjacency used for the IS-IS.
isis csnp-interval	Configures the interval at which periodic CSNP packets are sent on broadcast interfaces.
isis hello-interval	Specifies the length of time between consecutive hello packets sent by IS-IS.
isis hello-multiplier	Specifies the number of IS-IS hello packets a neighbor must miss before the ASA declares the adjacency as down.
isis hello padding	Configures IS-IS hellos to the full MTU size per interface.
isis lsp-interval	Configures the time delay between successive IS-IS LSP transmissions per interface.
isis metric	Configures the value of an IS-IS metric.
isis password	Configures the authentication password for an interface.
isis priority	Configures the priority of designated ASAs on the interface.
isis protocol shutdown	Disables the IS-IS protocol per interface.
isis retransmit-interval	Configures the amount of time between retransmission of each IS-IS LSP on the interface.
isis retransmit-throttle-interval	Configures the amount of time between retransmissions of each IS-IS LSP on the interface.
isis tag	Sets a tag on the IP address configured for an interface when the IP prefix is put into an LSP.
is-type	Assigns the routing level for the IS-IS routing process.
log-adjacency-changes	Enables the ASA to generate a log message when an NLSP IS-IS adjacency changes state (up or down).
lsp-full suppress	Configures which routes are suppressed when the PDU becomes full.
lsp-gen-interval	Customizes IS-IS throttling of LSP generation.
lsp-refresh-interval	Sets the LSP refresh interval.
max-area-addresses	Configures additional manual addresses for an IS-IS area.

Command	Description
max-lsp-lifetime	Sets the maximum time that LSPs persist in the ASA's database without being refreshed.
maximum-paths	Configures multi-path load sharing for IS-IS.
metric	Globally changes the metric value for all IS-IS interfaces.
metric-style	Configures an ASA running IS-IS so that it generates and only accepts new-style, length, value objects (TLVs).
net	Specifies the NET for the routing process.
passive-interface	Configures a passive interface.
prc-interval	Customizes IS-IS throttling of PRCs.
protocol shutdown	Disables the IS-IS protocol globally so that it cannot form any adjacency on any interface and will clear the LSP database.
redistribute isis	Redistributes IS-IS routes specifically from Level 1 into Level 2 or from Level 2 into Level 1.
route priority high	Assigns a high priority to an IS-IS IP prefix.
router isis	Enables IS-IS routing.
set-attached-bit	Specifies constraints for when a Level 1-Level 2 router should set its attached bit.
set-overload-bit	Configures the ASA to signal other routers not to use it as an intermediate hop in their SPF calculations.
show clns	Shows CLNS-specific information.
show isis	Shows IS-IS information.
show route isis	Shows IS-IS routes.
spf-interval	Customizes IS-IS throttling of SPF calculations.
summary-address	Creates aggregate addresses for IS-IS.

summary-address (router ospf)

To create aggregate addresses for OSPF, use the **summary-address** command in router ospf configuration mode. To remove the summary address or specific summary address options, use the **no** form of this command.

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]
no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

addr	Value of the summary address that is designated for a range of addresses.
mask	IP subnet mask that is used for the summary route.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Command Default

The defaults are as follows:

- *tag_value* is 0.
- Routes that match the specified prefix/mask pair are not suppressed.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Router configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Routes learned from other routing protocols can be summarized. Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

To remove a **summary-address** command from the configuration, use the no form of the command without specifying any of the optional keywords or arguments. To remove an option from a summary command in the configuration, use the **no** form of the command with the options that you want removed. See the "Examples" section for more information.

Examples

The following example configures route summarization with a **tag** set to 3:

```
ciscoasa(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
ciscoasa(config-router)#
```

The following example removes the **summary-address** command from the configuration:

```
ciscoasa(config-router)# no summary-address 1.1.0.0 255.255.0.0
ciscoasa(config-router)#
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
router ospf	Enters router configuration mode.
show ospf summary-address	Displays the summary address settings for each OSPF routing process.

sunrpc-server

To create entries in the SunRPC services table, use the **sunrpc-server** command in global configuration mode. To remove SunRPC services table entries from the configuration, use the **no** form of this command.

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp | udp**] **port** *port* [*-port*] **timeout** *hh:mm:ss*
no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp | udp**] **port** *port* [*-port*] **timeout** *hh:mm:ss*
no sunrpc-server *service_type* **server** *ip_addr*

Syntax Description

ifc_name	Server interface name.
ip_addr	SunRPC server IP address.
mask	Network mask.
port *port* [- *port*]	Specifies the SunRPC protocol port range.
port- *port*	(Optional) Specifies the SunRPC protocol port range.
protocol tcp	Specifies the SunRPC transport protocol.
protocol udp	Specifies the SunRPC transport protocol.
service	Specifies a service.
service_type	Sets the SunRPC service program number as specified in the **sunrpcinfo** command.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The SunRPC services table is used to allow SunRPC traffic through the ASA based on an established SunRPC session for the duration specified by the timeout.

Examples

The following example shows how to create an SunRPC services table:

```
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP port
 111 timeout 0:11:00
ciscoasa(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP port
 111 timeout 0:11:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the ASA.
show running-config sunrpc-server	Displays the information about the SunRPC configuration.

support-user-cert-validation

To validate a remote user certificate based on the current trustpoint, provided that this trustpoint is authenticated to the CA that issued the remote certificate, use the **support-user-cert-validation** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

support-user-cert-validation
no support-user-cert-validation

Syntax Description

This command has no arguments or keywords.

Command Default

The default setting is to support user certificate validation.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The ASA can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is automatically disabled if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and enables the trustpoint central to accept user validation:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# support-user-cert-validation
ciscoasa(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
default enrollment	Returns enrollment parameters to their defaults.

sw-module module password-reset

To reset the password on the software module to the default value, use the **sw-module module password-reset** command in privileged EXEC mode.

sw-module module *id* **password-reset**

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	This command was added.
9.1(1)	Support for the ASA CX software module was added with the **cxsc** keyword.

Usage Guidelines

After resetting the password, you should change it to a unique value using the module application. Resetting the module password causes the module to reboot. Services are not available while the module is rebooting, which may take several minutes. You can run the **show module** command to monitor the module state.

The command always prompts for confirmation. If the command succeeds, no other output appears. If the command fails, an error message appears that explains why the failure occurred.

This command is only valid when the module is in the Up state.

The default password depends on the module:

- ASA IPS—The default password is **cisco** for user cisco.
- ASA CX—The default password is **Admin123** for user admin.

Examples

The following example resets a password on the IPS module:

```
ciscoasa# sw-module module ips password-reset
Reset the password on module ips? [confirm] y
```

Related Commands

Command	Description
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module reset	Shuts down and reloads the module.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module recover

To load a recovery software image from disk for a software module, or to configure the image location, use the **sw-module module recover** command in privileged EXEC mode. You might need to recover a module using this command if, for example, the module is unable to load the current image.

sw-module module *id* **recover** { **boot | stop | configure image** *path* }

Syntax Description

id	Specifies the module ID, one of the following: • **sfr**—ASA FirePOWER module. • **ips**—IPS module • **cxsc**—ASA CX module
boot	Initiates recovery of this module and downloads a recovery image according to the **configure** settings. The module then reboots from the new image.
configure image *path*	Configures the new image location on the local disk, for example, disk0:image2.
stop	Stops the recovery action and deletes the image file for the module. You must enter this command within 30 seconds after starting recovery using the **sw-module module** *id* **recover boot** command. If you issue the **stop** command after this period, it might cause unexpected results, such as the module becoming unresponsive. If the module is already unresponsive, you might need to stop it before you can reboot it or apply a new image.

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	This command was added.
9.1(1)	Support for the ASA CX software module was added with the **cxsc** keyword.
9.2(1)	Support for the ASA FirePOWER module was added with the **sfr** keyword.

Usage Guidelines

Use this command install software modules. This can be a new module that is not yet configured on your device, or it can be an existing module that has suffered a failure, and you need to reinstall it.

When installing an image, use this command sequence:

- **sw-module module** *id* **configure image** *path* , to identify the location on disk0 of the software module image.
- **sw-module module** *id* **boot**, to boot that image.

You can boot an image only when the module is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information. If the module is not in an Up state, the ASA will forcefully shut down the module. A forced shutdown will destroy the old module disk image, including any configuration, and should only be used as a disaster recovery mechanism.

You can view the recovery configuration using the **show module** *id* **recover** command.

Note For the IPS module, do not use the **upgrade** command within the module software to install the image. See the chapters for each software module in the CLI configuration guide to learn how to complete the module installation and initial configuration.

Examples

The following example sets the module to download an image from disk0:image2:

```
ciscoasa# sw-module module ips recover configure image disk0:image2
```

The following example recovers the module:

```
ciscoasa# sw-module module ips recover boot
The module in slot ips will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot ips? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
sw-module module reset	Shuts down a module and performs a reset.
sw-module module reload	Reloads the module software.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module reload

To reload module software for a software module, use the **sw-module module reload** command in privileged EXEC mode.

sw-module module *id* **reload**

Syntax Description

id	Specifies the module ID, one of the following: • **sfr**—ASA FirePOWER module. • **ips**—IPS module • **cxsc**—ASA CX module

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	This command was added.
9.1(1)	Support for the ASA CX software module was added with the **cxsc** keyword.
9.2(1)	Support for the ASA FirePOWER module was added with the **sfr** keyword.

Usage Guidelines

This command differs from the **sw-module module reset** command, which also performs a reset before reloading the module.

This command is only valid when the module status is Up. See the **show module** command for state information.

Examples

The following example reloads the IPS module:

```
ciscoasa# sw-module module ips reload
Reload module in slot ips? [confirm] y
Reload issued for module in slot ips
%XXX-5-505002: Module in slot ips is reloading.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reset	Shuts down a module and performs a reset.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module reset

To reset the module and then reload the module software, use the **sw-module module reset** command in privileged EXEC mode.

sw-module module *id* **reset**

Syntax Description

id	Specifies the module ID, one of the following: • **sfr**—ASA FirePOWER module. • **ips**—IPS module • **cxsc**—ASA CX module

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	This command was added.
9.1(1)	Support for the ASA CX software module was added with the **cxsc** keyword.
9.2(1)	Support for the ASA FirePOWER module was added with the **sfr** keyword.

Usage Guidelines

When the module is in an Up state, the **sw-module module reset** command prompts you to shut down the software before resetting.

You can recover a module using the **sw-module module recover** command. If you enter the **sw-module module reset** command while the module is in a Recover state, the module does not interrupt the recovery process. The **sw-module module reset** command performs a reset of the module, and the module recovery continues after the reset. You might want to reset the module during recovery if the module hangs; a reset might resolve the issue.

This command differs from the **sw-module module reload** command, which only reloads the software and does not perform a reset.

This command is only valid when the module status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

Examples

The following example resets an IPS module that is in the Up state:

```
ciscoasa# sw-module module ips reset
The module in slot ips should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot ips? [confirm] y
Reset issued for module in slot ips
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
%XXX-5-505003: Module in slot ips is resetting.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module shutdown

To shut down the module software, use the **sw-module module shutdown** command in privileged EXEC mode.

sw-module module *id* **shutdown**

Syntax Description

id	Specifies the module ID, one of the following: • **sfr**—ASA FirePOWER module. • **ips**—IPS module • **cxsc**—ASA CX module

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	This command was added.
9.1(1)	Support for the ASA CX software module was added with the **cxsc** keyword.
9.2(1)	Support for the ASA FirePOWER module was added with the **sfr** keyword.

Usage Guidelines

Shutting down the module software prepares the module to be safely powered off without losing configuration data.

This command is only valid when the module status is Up or Unresponsive. See the **show module** command for state information.

Examples

The following example shuts down an IPS module:

```
ciscoasa# sw-module module ips shutdown
Shutdown module in slot ips? [confirm] y
Shutdown issued for module in slot ips
ciscoasa#
```

```
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module reset	Shuts down a module and performs a reset.
show module	Shows module information.

sw-module module uninstall

To uninstall a software module image and associated configuration, use the **sw-module module uninstall** command in privileged EXEC mode.

sw-module module *id* **uninstall**

Syntax Description

id	Specifies the module ID, one of the following: • **sfr**—ASA FirePOWER module. • **ips**—IPS module • **cxsc**—ASA CX module

Command Default

No default behavior or values.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
8.6(1)	We added this command.
9.1(1)	Support for the ASA CX software module was added with the **cxsc** keyword.
9.2(1)	Support for the ASA FirePOWER module was added with the **sfr** keyword.

Usage Guidelines

This command permanently uninstalls the software module image and associated configuration.

Examples

The following example uninstalls the IPS module image and configuration:

```
ciscoasa# sw-module module ips uninstall
Module ips will be uninstalled. This will completely remove the
disk image associated with the sw-module including any configuration
that existed within it.
Uninstall module <id>? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module reset	Shuts down a module and performs a reset.
show module	Shows module information.

switchport access vlan

To set the VLAN for an access mode switch port, use the **switchport access vlan** command in interface configuration mode. To revert to the default VLAN 1, use the **no** form of this command.

switchport access vlan *number*
no switchport access vlan *number*

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

vlan *number*	Specifies the VLAN ID to which you want to assign this switch port. The VLAN ID is between 1 and 4070 (Firepower 1010) or 4090 (ASA 5505).

Command Default

Firepower 1010: By default, Ethernet 0/1 through 0/7 are assigned to VLAN 1, and Ethernet 0/0 is assigned to VLAN 2.

Firepower 1010: By default, Ethernet1/2 through Ethernet 1/8 switch ports are in access mode and assigned to VLAN 1.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

Access ports accept only untagged traffic. The ASA tags traffic that enters the switch port with the VLAN that you specify so that the traffic can be forwarded to any other access port or trunk port on that same VLAN. The VLAN tag is removed when it egresses another access port, but is retained when it egresses a trunk port.

Note The ASA does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the ASA does not end up in a network loop.

ASA 5505

In transparent firewall mode, you can configure two active VLANs in the ASA 5505 Base license and three active VLANs in the Security Plus license, one of which must be for failover.

In routed mode, you can configure up to three active VLANs in the ASA 5505 Base license, and up to 20 active VLANs with the Security Plus license.

An active VLAN is a VLAN with a **nameif** command configured.

Examples

The following example assigns five ASA 5505 physical interfaces to three VLAN interfaces:

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport	Sets an interface to switch port mode.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport protected	Prevents a switch port from communicating with other switch ports on the same VLAN for extra security.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport

To set an interface to switch port mode, use the **switchport** command in interface configuration mode. To set the interface to firewall mode, use the **no** form of this command.

switchport
no switchport

Note Supported for the Firepower 1010 only.

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default for Ethernet 1/2 through 1/8.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

You can set each interface independently to be either a firewall interface or a switch port. By default, Ethernet 1/1 is a firewall interface, and the remaining Ethernet interfaces are configured as switch ports.

You cannot set the Management 1/1 interface to switch port mode.

If this interface is already in switchport mode, when you enter the **switchport** command, you are prompted for switch port parameters instead of changing the mode.

Examples

The following example sets Ethernet 1/3 and 1/4 to firewall mode:

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

Related Commands

Command	Description
forward interface	Disables forwarding from one VLAN to another.
interface vlan	Creates a VLAN interface for use with Firepower 1010 switch ports.
switchport	Sets an interface to switch port mode.
switchport access vlan	Identifies the VLAN for an access mode switch port.
switchport mode	Sets a switch port to access or trunk mode.
switchport trunk allowed vlan	Identifies the VLANs for a trunk mode switch port.

switchport mode

To set the switch port VLAN mode to either access (the default) or trunk, use the **switchport mode** command in interface configuration mode. To revert to the default access mode, use the **no** form of this command.

switchport mode { **access** | **trunk** }
no switchport mode { **access** | **trunk** }

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

access	Sets the switch port to access mode, which allows the switch port to pass traffic for only one VLAN. Only untagged packets are accepted. If a packet enters the switch port with a tag, the packet is dropped. Packets exit the switch port without an 802.1Q VLAN tag.
trunk	Sets the switch port to trunk mode, so it can pass traffic for multiple VLANs. Tagged and untagged packets are accepted. Packets exit the switch port with an 802.1Q VLAN tag. If a packet enters the switch port without a tag, it is assigned to the native VLAN.

Command Default

By default, the mode is access.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
7.2(2)	You can now configure multiple trunk ports, rather than being limited to one trunk.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

After you set the mode to access mode, use the **switchport vlan access** command to identify the VLAN.

After you set the mode to trunk mode, use the **switchport trunk allowed vlan** command to assign multiple VLANs to the trunk. If you set the mode to trunk mode, and you have not yet configured the **switchport trunk allowed vlan** command, the switch port remains in “line protocol down” state, and cannot participate in traffic forwarding. For the ASA 5505, trunk mode is available only with the Security Plus license.

Examples

The following example configures an access mode switch port assigned to VLAN 100, and a trunk mode switch port assigned to VLANs 200 and 300:

```
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200,300
ciscoasa(config-if)# no shutdown
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport	Sets an interface to switch port mode.
switchport access vlan	Assigns the switch port to a VLAN.
switchport protected	Prevents a switch port from communicating with other switch port on the same VLAN for extra security.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport monitor

To enable SPAN switch port monitoring, use the **switchport monitor** command in interface configuration mod. The port for which you enter this command (called the destination port) receives a copy of every packet transmitted or received on the specified source port. The SPAN feature lets you attach a sniffer to the destination port so you can monitor traffic. You can specify multiple source ports by entering this command multiple times. You can only enable SPAN for one destination port. To disable monitoring of a source port, use the **no** form of this command.

switchport monitor *source_port* [**tx** | **rx** | **both**]
no switchport monitor *source_port* [**tx** | **rx** | **both**]

Note Supported for the ASA 5505 only.

Syntax Description

both	(Optional) Specifies that both transmitted and received traffic is monitored. **both** is the default.
rx	(Optional) Specifies that only received traffic is monitored.
source_port	Specifies the port you want to monitor. You can specify any Ethernet port as well as the Internal-Data0/1 backplane port that passes traffic between VLAN interfaces. Because the Internal-Data0/1 port is a Gigabit Ethernet port, you might overload the Fast Ethernet destination port with traffic. Monitor the port Internal-Data0/1 with caution.
tx	(Optional) Specifies that only transmitted traffic is monitored.

Command Default

The default type of traffic to monitor is **both**.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

If you do not enable SPAN, then attaching a sniffer to one of the switch ports only captures traffic to or from that port. To capture traffic to or from multiple ports, you need to enable SPAN and identify the ports you want to monitor.

Use caution while connecting a SPAN destination port to another switch, as it could result in network loops.

Examples

The following example configures the Ethernet 0/1 port as the destination port which monitors the Ethernet 0/0 and Ethernet 0/2 ports:

```
ciscoasa(config)# interface ethernet 0/1
ciscoasa(config-if)# switchport monitor ethernet 0/0
ciscoasa(config-if)# switchport monitor ethernet 0/2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport protected	Prevents a switch port from communicating with other switch port on the same VLAN for extra security.

switchport protected

To prevent a switch port from communicating with other protected switch ports on the same VLAN, enter the **switchport protected** command in interface configuration mode. This feature provides extra security to the other switch ports on a VLAN if one switch port becomes compromised. To disable protected mode, use the **no** form of this command.

switchport protected
no switchport protected

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the interfaces are not protected.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Communication to and from unprotected ports is not restricted by this command.

Examples

The following example configures seven switch ports. The Ethernet 0/4, 0/5, and 0/6 are assigned to the DMZ network and are protected from each other.

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/5
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/6
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport trunk

To assign VLANs to a trunk port, use the **switchport trunk** command in interface configuration mode. Use the **no** form of the command to remove a VLAN from the trunk.

switchport trunk { **allowed vlans** *vlan_range* **| native vlan** *vlan* }
no switchport trunk { **allowed vlans** *vlan_range* **| native vlan** *vlan* }

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

allowed vlans *vlan_range*	Identifies one or more VLANs that you can assign to the trunk port. The VLAN ID is between 1 and 4070 (Firepower 1010) or 4090 (ASA 5505). The *vlan_range* can be identified in one of the following ways: • A single number (n) • A range (n-x) Separate numbers and ranges by commas, for example: 5,7-10,13,45-100 You can enter spaces instead of commas, but the command is saved to the configuration with commas. If you include the native VLAN in this command, it is ignored; the trunk port always removes the VLAN tagging when sending native VLAN traffic out of the port. Moreover, it will not receive traffic that still has native VLAN tagging.
native vlan *vlan*	Assigns a native VLAN to the trunk. When the trunk receives untagged traffic, it tags it to the native VLAN ID so that the ASA can forward the traffic to the correct switch ports, or can route it to another firewall interface. When the ASA sends native VLAN ID traffic out of the trunk port, it removes the VLAN tag. Be sure to set the same native VLAN on the trunk port on the other switch so that the untagged traffic will be tagged to the same VLAN. Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.

Command Default

By default, no VLANs are assigned to the trunk.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Interface configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.
7.2(2)	This command was modified to allow more than 3 VLANs per switch port. Also, you can now configure multiple trunk ports, instead of being limited to only one. This command also uses commas instead of spaces to separate VLAN IDs.
7.2(4)/8.0(4)	Native VLAN support was added with the **native vlan** keywords.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

If you want to create a trunk port to pass multiple VLANs on the switch port, set the mode to trunk mode using the **switchport mode trunk** command, and then use the **switchport trunk** command to assign VLANs to the trunk. This switch port cannot pass traffic until you assign at least one VLAN to it. If you set the mode to trunk mode, and you have not yet configured the **switchport trunk allowed vlan** command, the switch port remains in "line protocol down" state and cannot participate in traffic forwarding.

ASA 5505

Trunk mode is available only with the Security Plus license.

Note This command is not downgrade-compatible to Version 7.2(1); the commas separating the VLANs are not recognized in 7.2(1). If you downgrade, be sure to separate the VLANs with spaces, and do not exceed the 3 VLAN limit.

Examples

The following example configures seven VLAN interfaces, including the failover interface which is configured using the **failover lan** command. VLANs 200, 201, and 202 are trunked on Ethernet 0/1.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 201
ciscoasa(config-if)# nameif dept1
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 202
ciscoasa(config-if)# nameif dept2
ciscoasa(config-if)# security-level 90
ciscoasa(config-if)# ip address 10.2.3.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 200-202
ciscoasa(config-if)# switchport trunk native vlan 5
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport protected	Prevents a switch port from communicating with other switch ports on the same VLAN for extra security.

synack-data

To set the action for TCP SYNACK packets that contain data, use the **synack-data** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

synack-data { **allow** | **drop** }
no synack-data

Syntax Description

allow	Allows TCP SYNACK packets that contain data.
drop	Drops TCP SYNACK packets that contain data.

Command Default

The default action is to drop TCP SYNACK packets that contain data.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was added.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
    a. **synack-data**—In tcp-map configuration mode, you can enter the **synack-data** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
    a. **class**—Identify the class map on which you want to perform actions.
    b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example sets the ASA to allow TCP SYNACK packets that contain data:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# synack-data allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

synchronization

To enable the synchronization between BGP and your Interior Gateway Protocol (IGP) system, use the synchronization command in address family configuration mode. To enable the Cisco IOS software to advertise a network route without waiting for the IGP, use the no form of this command.

synchronization
no synchronization

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Address-family configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
9.2(1)	This command was added.

Usage Guidelines

Usually, a BGP speaker does not advertise a route to an external neighbor unless that route is local or exists in the IGP. By default, synchronization between BGP and the IGP is turned off to allow the Cisco IOS software to advertise a network route without waiting for route validation from the IGP. This feature allows routers and access servers within an autonomous system to have the route before BGP makes it available to other autonomous systems.

Use the synchronization command if routers in the autonomous system do not speak BGP.

Examples

The following example shows how to enable synchronization in address family configuration mode. The router validates the network route in its IGP before advertising the route externally.

```
ciscoasa(config)# router bgp 65120
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# synchronization
```

syn-data

To allow or drop SYN packets with data, use the **syn-data** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

syn-data { **allow | drop** }
no syn-data { **allow | drop** }

Syntax Description

allow	Allows SYN packets that contain data.
drop	Drops SYN packets that contain data.

Command Default

Packets with SYN data are allowed by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tcp-map configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **syn-data** command in tcp-map configuration mode to drop packets with data in SYN packets.

According to the TCP specification, TCP implementations are required to accept data contained in a SYN packet. Because this is a subtle and obscure point, some implementations may not handle this correctly. To avoid any vulnerabilities to insertion attacks involving incorrect end-system implementations, you may choose to drop packets with data in SYN packets.

Examples

The following example shows how to drop SYN packets with data on all TCP flows:

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# syn-data drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

sysopt connection permit-vpn

For traffic that enters the ASA through a VPN tunnel and is then decrypted, use the **sysopt connection permit-vpn** command in global configuration mode to allow the traffic to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. To disable this feature, use the **no** form of this command.

sysopt connection permit-vpn
no sysopt connection permit-vpn

outputclass="syntax">

This command has no arguments or keywords.

Command Default

This feature is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command is now enabled by default. Also, only interface access lists are bypassed; group policy or per-user access lists remain in force.
7.1(1)	This command was changed from **sysopt connection permit-ipsec**.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

By default, the ASA allows VPN traffic to terminate on an ASA interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an interface access list. By default, you also do not need an interface access list for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the ASA performance without any security risks. (Group policy and per-user authorization access lists still apply to the traffic.)

You can require an interface access list to apply to the local IP addresses by entering the **no sysopt connection permit-vpn** command. See the **access-list** and **access-group** commands to create an access list and apply it to an interface. The access list applies to the local IP address, and not to the original client IP address used before the VPN packet was decrypted.

Note For route-based VPNs, this command is ignored. You must always create access control rules to allow route-based VPN traffic.

Examples

The following example requires decrypted VPN traffic to comply with interface access lists:

```
ciscoasa(config)# no
 sysopt connection permit-vpn
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection preserve-vpn-flows

To preserve and resume stateful (TCP) tunneled IPsec LAN-to-LAN traffic within the timeout period after the tunnel drops and recovers, use the **sysopt connection preserve-vpn-flows** command. To disable this feature, use the **no** form of this command.

sysopt connection preserve-vpn-flows
no sysopt connection preserve-vpn-flows

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

With the persistent IPsec tunneled flows feature enabled, as long as the tunnel is recreated within the timeout window, data continues flowing successfully because the security appliance still has access to the state information in the original flow.

This command supports only IPsec LAN-to-LAN tunnels, including Network Extension Mode. It does not support AnyConnect/SSL VPN or IPsec remote-access tunnels.

Examples

The following example specifies that the state information for the tunnel will be preserved and the tunneled IPsec LAN-to-LAN VPN traffic will resume after the tunnel drops and is reestablished within the timeout period:

```
ciscoasa(config)# no sysopt connection preserve-vpn-flows
```

To see whether this feature is enabled, enter the show run all command for sysopt:

```
ciscoasa(config)# show run all sysopt
```

A sample result follows. For illustrative purposes, in this and all following examples, the preserve-vpn-flows item is bolded:

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

To reclassify existing VPN flows, use the **sysopt connection reclassify-vpn** command in global configuration mode. To disable this feature, use the **no** form of this command.

sysopt connection reclassify-vpn
no sysopt connection reclassify-vpn

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	—	• Yes	• Yes	—

Command History

Release	Modification
8.0(2)	This command was added
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When a new IPsec Phase 2 Security Association (SA) of a VPN tunnel comes up, this command tears down existing flows that match the new SA to ensure that existing flows that need encryption get torn down, recreated and encrypted.

If the command is disabled, an existing connection that requires encryption will have to be cleared manually (for example, using clear conn addr x.x.x.x port xx) in order to be re-established and go through the new VPN tunnel.

This command only applies for LAN-to-LAN and dynamic VPNs. This command has no effect on EZVPN or VPN client connections.

Examples

The following example enables VPN reclassification:

```
ciscoasa(config)# sysopt connection reclassify-vpn
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.

Command	Description
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-vpn	Permits any packets that come from an IPsec tunnel without checking any access lists for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection tcp-max-unprocessed-seg

To configure the maximum number of TCP unprocessed segments, use the **sysopt connection tcp-max-unprocessed-seg** command in global configuration mode. To restore the default setting, use the **no** form of this command.

sysopt connection tcp-max-unprocessed-seg *segments*
no sysopt connection tcp-max-unprocessed-seg *segments*

Syntax Description

segments	Sets the maximum number of TCP unprocessed segments, from 6 to 24.

Command Default

No command default, but the default number of unprocessed segments is 6.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
9.19(1)	This command was added. It is also available in point releases from release 9.12 and higher.

Usage Guidelines

If you find that SIP phones are not connecting to the call manager, you can try increasing the maximum number of unprocessed TCP segments using this command. The default is 6, so try a higher number.

Example

The following example sets the maximum number of unprocessed segments to 24.

```
ciscoasa(config)# sysopt connection tcp-max-unprocessed-seg 24
```

sysopt connection tcpmss

To ensure that the maximum TCP segment size for through traffic does not exceed the value you set and that the maximum is not less than a specified size, use the **sysopt connection tcpmss** command in global configuration mode. To restore the default setting, use the **no** form of this command.

sysopt connection tcpmss [**minimum**] *bytes*
no sysopt connection tcpmss [**minimum**] [*bytes*]

Syntax Description

bytes	Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting *bytes* to 0. For the **minimum** keyword, the *bytes* represent the smallest maximum value allowed.
minimum	Overrides the maximum segment size to be no less than *bytes*, between 48 and 65535 bytes. This feature is disabled by default (set to 0).

Command Default

By default, the maximum TCP MSS on the ASA is 1380 bytes. This default accommodates IPv4 IPsec VPN connections where the headers can equal up to 120 bytes; this value fits within the default MTU of 1500 bytes.

The minimum feature is disabled by default (set to 0).

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The TCP maximum segment size (MSS) is the size of the TCP payload before any TCP and IP headers are added. UDP packets are not affected. The client and the server exchange TCP MSS values during the three-way handshake when establishing the connection.

You can set the TCP MSS on the ASA for through traffic; by default, the maximum TCP MSS is set to 1380 bytes. This setting is useful when the ASA needs to add to the size of the packet for IPsec VPN encapsulation. However, for non-IPsec endpoints, you should disable the maximum TCP MSS on the ASA.

If you set a maximum TCP MSS, if either endpoint of a connection requests a TCP MSS that is larger than the value set on the ASA, then the ASA overwrites the TCP MSS in the request packet with the ASA maximum. If the host or server does not request a TCP MSS, then the ASA assumes the RFC 793-default value of 536 bytes (IPv4) or 1220 bytes (IPv6), but does not modify the packet. For example, you leave the default MTU as 1500 bytes. A host requests an MSS of 1500 minus the TCP and IP header length, which sets the MSS to

1460. If the ASA maximum TCP MSS is 1380 (the default), then the ASA changes the MSS value in the TCP request packet to 1380. The server then sends packets with 1380-byte payloads. The ASA can then add up to 120 bytes of headers to the packet and still fit in the MTU size of 1500.

You can also configure the minimum TCP MSS; if a host or server requests a very small TCP MSS, the ASA can adjust the value up. By default, the minimum TCP MSS is not enabled.

For to-the-box traffic, including for SSL VPN connections, this setting does not apply. The ASA uses the MTU to derive the TCP MSS: MTU - 40 (IPv4) or MTU - 60 (IPv6).

The default TCP MSS assumes the ASA acts as an IPv4 IPsec VPN endpoint and has an MTU of 1500. When the ASA acts as an IPv4 IPsec VPN endpoint, it needs to accommodate up to 120 bytes for TCP and IP headers.

If you change the MTU value, use IPv6, or do not use the ASA as an IPsec VPN endpoint, then you should change the TCP MSS setting. See the following guidelines:

- Normal traffic—Disable the TCP MSS limit and accept the value established between connection endpoints. Because connection endpoints typically derive the TCP MSS from the MTU, non-IPsec packets usually fit this TCP MSS.
- IPv4 IPsec endpoint traffic—Set the maximum TCP MSS to the MTU - 120. For example, if you use jumbo frames and set the MTU to 9000, then you need to set the TCP MSS to 8880 to take advantage of the new MTU.
- IPv6 IPsec endpoint traffic—Set the maximum TCP MSS to the MTU - 140.

Examples

The following example enables jumbo frames, increases the MTU on all interfaces, and disables the TCP MSS for non-VPN traffic (by setting the TCP MSS to 0, which means there is no limit):

```
ciscoasa(config)# jumbo frame-reservation
ciscoasa(config)# mtu inside 9198
ciscoasa(config)# mtu outside 9198
ciscoasa(config)# sysopt connection tcpmss 0
```

The following example enables jumbo frames, increases the MTU on all interfaces, and changes the TCP MSS for VPN traffic to 9078 (the MTU minus 120):

```
ciscoasa(config)# jumbo frame-reservation
ciscoasa(config)# mtu inside 9198
ciscoasa(config)# mtu outside 9198
ciscoasa(config)# sysopt connection tcpmss 9078
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPsec tunnel without checking any ACLs for interfaces.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection timewait

To force each TCP connection to linger in a shortened TIME_WAIT state of at least 15 seconds after the final normal TCP close-down sequence, use the **sysopt connection timewait** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to use this feature if an end host application default TCP terminating sequence is a simultaneous close.

sysopt connection timewait
no sysopt connection timewait

Note An RST packet (not a normal TCP close-down sequence) received in FIN_WAIT2 state, will also trigger the 15 second delay. The ASA holds on to the connection for 15 seconds after receiving the last packet (either FIN/ACK or RST) of the connection.

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The default behavior of the ASA is to track the shutdown sequence and release the connection after two FINs and the ACK of the last FIN segment. This quick release heuristic enables the ASA to sustain a high connection rate, based on the most common closing sequence, known as the normal close sequence. However, in a simultaneous close, both ends of the transaction initiate the closing sequence, as opposed to the normal close sequence where one end closes and the other end acknowledges prior to initiating its own closing sequence (see RFC 793). Thus, in a simultaneous close, the quick release forces one side of the connection to linger in the CLOSING state. Having many sockets in the CLOSING state can degrade the performance of an end host. For example, some WinSock mainframe clients are known to exhibit this behavior and degrade the performance of the mainframe server. Using the **sysopt connection timewait** command creates a window for the simultaneous close down sequence to complete.

Examples

The following example enables the timewait feature:

```
ciscoasa(config)# sysopt connection timewait
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPsec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.

sysopt noproxyarp

To disable proxy ARP for NAT global addresses or VPN client addresses on an interface, use the **sysopt noproxyarp** command in global configuration mode. To reenable proxy ARP, use the **no** form of this command.

sysopt noproxyarp *interface_name*
no sysopt noproxyarp *interface_name*

Syntax Description

interface_name	The interface name for which you want to disable proxy ARP.

Command Default

Proxy ARP is enabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.0(3)	This command was extended to affect VPN proxy ARPs when the VPN client addresses overlap with an internal network.

Usage Guidelines

If you have a VPN client address pool that overlaps with an existing network, the ASA by default sends proxy ARPs on all interfaces. If you have another interface that is on the same Layer 2 domain, it will see the ARP requests and will answer with the MAC address of its interface. The result of this is that the return traffic of the VPN clients towards the internal hosts will go to the wrong interface and will get dropped. In this case, you need to enter the **sysopt noproxyarp** command for the interface where you do not want proxy ARPs.

In rare circumstances, you might want to disable proxy ARP for NAT global addresses.

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking "Who is this IP address?" The device owning the IP address replies, "I own that IP address; here is my MAC address."

Proxy ARP is when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The ASA uses proxy ARP when you configure NAT and specify a global address that is on the same network as the ASA interface. The only way traffic can reach the hosts is if the ASA uses proxy ARP to claim that the ASA MAC address is assigned to destination global addresses.

Examples

The following example disables proxy ARP on the inside interface:

```
ciscoasa(config)# sysopt noproxyarp inside
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

sysopt radius ignore-secret

To ignore the authentication key in RADIUS accounting responses, use the **sysopt radius ignore-secret** command in global configuration mode. To disable this feature, use the **no** form of this command. You might need to ignore the key for compatibility with some RADIUS servers.

sysopt radius ignore-secret
no sysopt radius ignore-secret

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Some RADIUS servers fail to include the key in the authenticator hash within the accounting acknowledgment response. This usage caveat can cause the ASA to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to ignore the key in these acknowledgments, thus avoiding the retransmit problem. (The key identified here is the same one you set with the **aaa-server host** command.)

Examples

The following example ignores the authentication key in accounting responses:

```
ciscoasa(config)# sysopt radius ignore-secret
```

Related Commands

Command	Description
aaa-server host	Identifies a AAA server.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

sysopt traffic detailed-statistics

To calculate per-second per-protocol detailed statistics for the changed traffic system options, use the **sysopt traffic detailed-statistics** command in global configuration mode. To disable this feature, use the **no** form of this command.

sysopt traffic detailed-statistics
no sysopt traffic detailed-statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This feature is disabled by default.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

Use the **sysopt traffic detailed-statistics** command to calculate per-second per-protocol detailed statistics for the changed traffic system options.

Examples

The following example displays detailed statistics for changed traffic system options:

```
ciscoasa(config)# sysopt traffic detailed-statistics
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.