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.