



CHAPTER **29**

show service-policy through show xlate Commands

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 | inspect | ips | police | priority | shape]
```

```
show service-policy [global | interface intf] [set connection [details]]
```

```
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) Limits the output to policies that include the csc command.
<i>dest_ip dest_mask</i>	The destination IP address and netmask of the traffic flow.
details	(Optional) Displays per-client connection information, if a per-client connection limit is enabled.
eq dest_port	(Optional) The equals operator, requiring the destination port to match the port number that follows.
eq src_port	(Optional) The equals operator, requiring the source port to match the port number that follows.
flow protocol	(Optional) Specifies a traffic flow for which you want to see the policies that the adaptive security appliance would apply to the flow. The arguments and keywords following the flow keyword specify the flow in ip-5-tuple format. Valid values for the <i>protocol</i> argument are listed in the “Usage Guidelines” section, below.
global	(Optional) Limits output to the global policy, which applies to all interfaces.
host dest_host	The host destination IP address of the traffic flow.
host src_host	The host source IP address of the traffic flow.
<i>icmp_control_message</i>	(Optional) Specifies an ICMP control message of the traffic flow. Valid values for the <i>icmp_control_message</i> argument are listed in the “Usage Guidelines” section, below.
<i>icmp_number</i>	(Optional) Specifies the ICMP protocol number of the traffic flow.
inspect	(Optional) Limits the output to policies that include an inspect command.
interface intf	(Optional) Displays policies applied to the interface specified by the <i>intf</i> argument, where <i>intf</i> is the interface name given by the nameif command.
ips	Limits output to policies that include the ips command.
police	Limits output to policies that include the police command.
priority	Limits output to policies that include the priority command.
set connection	Limits output to policies that include the set connection command.
shape	Limits output to policies that include the shape command.
<i>src_ip src_mask</i>	The source IP address and netmask used in the traffic flow.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The csc keyword was added.
7.2(4)/8.0(4)	The shape keyword was added.

Usage Guidelines

The **flow** keyword lets you determine, for any flow that you can describe, the policies that the adaptive security appliance would apply to that flow. You can use this to check that your service policy configuration will provide the services you want for specific connections. The arguments and keywords following the **flow** keyword specifies the flow in ip-5-tuple format with no object grouping.

Because the flow is described in ip-5-tuple format, not all match criteria are supported. Following are the list of match criteria that are supported for flow match:

- **match access-list**
- **match port**
- **match rtp**
- **match default-inspection-traffic**

The **priority** keyword is used to display the aggregate counter values of packets transmitted through an interface.

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.

protocol Argument Values

The following are valid values for the *protocol* argument:

- *number*—The protocol number (0 - 255).
- **ah**
- **eigrp**
- **esp**
- **gre**
- **icmp**
- **icmp6**
- **igmp**

- **igrp**
- **ip**
- **ipinip**
- **ipsec**
- **nos**
- **ospf**
- **pcp**
- **pim**
- **pptp**
- **snp**
- **tcp**
- **udp**

icmp_control_message Argument Values

The following are valid values for the *icmp_control_message* argument:

- **alternate-address**
- **conversion-error**
- **echo**
- **echo-reply**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **parameter-problem**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **unreachable**

Examples

The following is sample output from the **show service-policy global** command:

```
hostname# 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:

```

hostname# 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:

```

hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq 5060

Global policy:
  Service-policy: fl_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.

```

hostname# 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

```

The following is sample output from the **show service-policy inspect waas** command. This example shows the waas statistics.

```
hostname# 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
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy 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 service-policy inspect ftp

To display the FTP configuration for FTP inspection, use the **show service-policy inspect ftp** command in privileged EXEC mode.

show service-policy [interface *int*] inspect ftp

Syntax Description.

interface *int* (Optional) Identifies a specific interface.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

During FTP inspection, the adaptive security appliance can drop packets silently. To see whether the adaptive security appliance has dropped any packets internally, enter the **show service-policy inspect ftp** command.



Note

The command output does not display drop counters that are zero. The adaptive security appliance infrequently drops packets silently; therefore, the output of this command rarely displays drop counters.

[Table 29-1](#) describes the output from the **show service-policy inspect ftp** command:

Table 29-1 FTP Drop Counter Descriptions

Drop Counter	Counter increments...
Back port is zero drop	If the port value is 0 when processing APPE, STOR, STOU, LIST, NLIST, RETR commands.
Can't allocate back conn drop	When an attempt to allocate a secondary data connection fails.
Can't allocate CP conn drop	When the adaptive security appliance attempts to allocate a data structure for a CP connection and the attempt fails. Check for low system memory.

Table 29-1 FTP Drop Counter Descriptions

Drop Counter	Counter increments...
Can't alloc FTP data structure drop	When the adaptive security appliance attempts to allocate a data structure for FTP inspection and the attempt fails. Check for low system memory
Can't allocate TCP proxy drop	When the adaptive security appliance attempts to allocate a data structure for a TCP proxy and the attempt fails. Check for low system memory
Can't append block drop	When the FTP packet is out of space and data cannot be added to the packet.
Can't PAT port drop	When the adaptive security appliance fails to configure PAT for a port.
Cmd in reply mode drop	When a command is received in REPLY mode.
Cmd match failure drop	When the adaptive security appliance encounters an internal error in regex matching. Contact Cisco TAC.
Cmd not a cmd drop	When the FTP command string contains invalid characters, such as numeric characters.
Cmd not port drop	When the adaptive security appliance expects to receive a PORT command but receives another command.
Cmd not supported drop	When the adaptive security appliance encounters an unsupported FTP command.
Cmd not supported in IPv6 drop	When an FTP command is not supported in IPv6.
Cmd not terminated drop	When the FTP command is not terminated with NL or CR.
Cmd retx unexpected drop	When a retransmitted packet is received unexpectedly.
Cmd too short drop	When the FTP command is too short.
ERPT too short drop	When the ERPT command is too short.
IDS internal error drop	When an internal error is encountered during FTP ID checks. Contact Cisco TAC.
Invalid address drop	When an invalid IP address is encountered during inspection.
Invalid EPSV format drop	When a formatting error is found in the ESPV command.
Invalid ERPT AF number drop	When the Address Family (AF) is invalid in the ERPT command.
Invalid port drop	When an invalid port is encountered during inspection.
No back port for data drop	If the packet does not contain a port when processing APPE, STOR, STOU, LIST, NLIST, RETR commands.
PORT command/reply too long drop	When the length of PORT command or passive reply is greater than 8.
Reply code invalid drop	When the reply code is invalid.
Reply length negative drop	When a reply has a negative length value.
Reply unexpected drop	If the adaptive security appliance receives a reply when a reply is not expected.

Table 29-1 FTP Drop Counter Descriptions

Drop Counter	Counter increments...
Retx cmd in cmd mode drop	When a retransmitted command is received in CMD mode.
Retx port not old port drop	When a packet is retransmitted but the port in the packet is different from the originally transmitted port.
TCP option exceeds limit drop	When the length value in a TCP option causes the length of the option to exceed the TCP header limit.
TCP option length error drop	When the length value in a TCP option is not correct.

Examples

The following is sample output from the **show service-policy inspect ftp** command:

```
hostname# show show show service-policy inspect ftp

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: ftp, packet 0, drop 0, reset-drop 0
              Can't alloc CP conn drop 1, Can't alloc proxy drop 2
              TCP option exceeds limit drop 3, TCP option length error drop 4
              Can't alloc FTP structure drop 1, Can't append block drop 2
              PORT cmd/reply too long drop 3, ERPT too short drop 4
              Invalid ERPT AF number drop 5, IDS internal error drop 6
              Invalid address drop 7, Invalid port drop 8
              Can't PAT port drop 9, Invalid EPSV format drop 10
              Retx port not old port drop 11, No back port for data drop 12
              Can't alloc back conn drop 13, Back port is zero drop 14
              Cmd too short drop 15, Cmd not terminated drop 16
              Cmd not a cmd drop 17, Cmd match failure drop 18
              Cmd not supported drop 19, Cmd not supported in IPv6 drop 20
              Cmd not port drop 21, Retx cmd in cmd mode drop 22
              Cmd retx unexpected drop 23, Cmd in reply mode drop 24
              Reply length negative drop 25, Reply unexpected drop 26
              Reply code invalid drop 27
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ftp	Configures application inspection to inspect FTP traffic.

show service-policy inspect gtp

To display the GTP configuration, use the **show service-policy inspect gtp** command in privileged EXEC mode.

```
show service-policy [interface int] inspect gtp {pdp-context [apn ap_name | detail | imsi
  IMSI_value | ms-addr IP_address | tid tunnel_ID | version version_num ] | pdpmcb | requests
  | statistics [gsn IP_address] }
```

Syntax Description.

apn	(Optional) Displays the detailed output of the PDP contexts based on the APN specified.
<i>ap_name</i>	Identifies the specific access point name for which statistics are displayed.
detail	(Optional) Displays the detailed output of the PDP contexts.
imsi	Displays the detailed output of the PDP contexts based on the IMSI specified.
<i>IMSI_value</i>	Hexadecimal value that identifies the specific IMSI for which statistics are displayed.
interface	(Optional) Identifies a specific interface.
<i>int</i>	Identifies the interface for which information will be displayed.
gsn	(Optional) Identifies the GPRS support node, which is interface between the GPRS wireless data network and other networks.
gtp	(Optional) Displays the service policy for GTP.
<i>IP_address</i>	IP address for which statistics are displayed.
ms-addr	(Optional) Displays the detailed output of the PDP contexts based on the MS Address specified.
pdp-context	(Optional) Identifies the Packet Data Protocol context
pdpmcb	(Optional) Displays the status of the PDP master control block.
requests	(Optional) Displays status of GTP requests.
statistics	(Optional) Displays GTP statistics.
tid	(Optional) Displays the detailed output of the PDP contexts based on the TID specified.
<i>tunnel_ID</i>	Hexadecimal value that identifies the specific tunnel for which statistics are displayed.
version	(Optional) Displays the detailed output of the PDP contexts based on the GTP version.
<i>version_num</i>	Specifies the version of the PDP context for which statistics are displayed. The valid range is 0 to 255.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can use the vertical bar | to filter the display. Type | for more display filtering options.

The **show pdp-context** command displays PDP context-related information.

The Packet Data Protocol context is identified by the tunnel ID, which is a combination of IMSI and NSAPI. A GTP tunnel is defined by two associated PDP Contexts in different GSN nodes and is identified with a Tunnel ID. A GTP tunnel is necessary to forward packets between an external packet data network and a mobile station user.

The **show gtp requests** command displays current requests in the request queue.

Examples

The following is sample output from the **show gtp requests** command:

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

You can use the vertical bar | to filter the display, as in the following example:

```
hostname# show service-policy gtp statistics | grep gsn
```

This example shows the GTP statistics with the word gsn in the output.

The following command shows the statistics for GTP inspection:

```
hostname# 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 | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total_created_pdp | 0 | total_deleted_pdp | 0
  total_created_pdpmb | 0 | total_deleted_pdpmb | 0
  pdp_non_existent | 0
```

The following command displays information about the PDP contexts:

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13 | gprs.cisco.com

| user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
| primary pdp: Y | nsapi: 2
| sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
| ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
| sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
| ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
| seq_tpdu_up: | 0 | seq_tpdu_down: | 0
| signal_sequence: | 0
| upstream_signal_flow: | 0 | upstream_data_flow: | 0
| downstream_signal_flow: | 0 | downstream_data_flow: | 0
| RAupdate_flow: | 0
```

Table 29-2 describes each column the output from the `show service-policy inspect gtp pdp-context` command.

Table 29-2 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	Displays the serving gateway service node.
Idle	Displays the time for which the PDP context has not been in use.
APN	Displays the access point name.

Related Commands

Commands	Description
<code>class-map</code>	Defines the traffic class to which to apply security actions.
<code>clear service-policy inspect gtp</code>	Clears global GTP statistics.
<code>debug gtp</code>	Displays detailed information about GTP inspection.
<code>gtp-map</code>	Defines a GTP map and enables GTP map configuration mode.
<code>inspect gtp</code>	Applies a specific GTP map to use for application inspection.

show service-policy inspect radius-accounting

To display the Radius-accounting configuration for application inspection, use the **show service-policy inspect radius-accounting** command in privileged EXEC mode.

show service-policy [interface *int*] inspect radius-accounting

Syntax Description. **interface *int*** (Optional) Identifies a specific interface.

Defaults No default behavior or values.

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples The following is sample output from the **show show service-policy inspect radius-accounting** command:

```
hostname# show show service-policy inspect radius-accounting
0 in use, 0 most used, 200 maximum allowed
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect radius-accounting	Configures application inspection to inspect Radius accounting traffic.

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	Keyword	Description
	backup	(Optional) Shows information about the backup server.
	client	(Optional) Limits the display to participants.
	detail	(Optional) Shows all statistics, including per participant.
	<i>hostname</i>	(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	•	—	•	—	—

Command History	Release	Modification
	8.2(1)	This command was introduced.

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:

```
hostname> 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

```

The following is sample output from the **show shared license detail** command on the license server:

```

hostname> 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       : XXXXXXXXXXXX
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.

Command	Description
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.
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		
<i>src_ip</i>	(Optional)	Displays the information for that address.
<i>statistics</i>	(Optional)	Displays the interface counters only.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.
	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:

```
hostname# 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show sip** command assists in troubleshooting SIP inspection engine issues and is described with the **inspect protocol sip udp 5060** command. The **show timeout sip** command displays the timeout value of the designated protocol.

The **show sip** command displays information for SIP sessions established across the adaptive security appliance. Along with the **debug sip** and **show local-host** commands, this command is used for troubleshooting SIP inspection engine issues.



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:

```
hostname# 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 adaptive security appliance (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
class-map	Defines the traffic class to which to apply security actions.
debug sip	Enables debug information for SIP.
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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show skinny** command assists in troubleshooting SCCP (Skinny) inspection engine issues.

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 adaptive security appliance. 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.

```
hostname# show skinny
```

```

          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.

The following is the xlate information for these Skinny connections:

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D|DNS, d|dump, I|identity, i|inside, n|no random,
      |o|outside, r|portmap, s|static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
debug skinny	Enables SCCP debug information.
inspect skinny	Enables SCCP 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 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.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

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.

```
hostname> 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:
```

```
hostname# 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	<i>sla-id</i>	(Optional) The ID number of the SLA operation. Valid values are from 1 to 2147483647.
---------------------------	---------------	---

Defaults 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	•	•	•	•	—

Command History	Release	Modification
	7.2(1)	This command was introduced.

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:

```
hostname> show sla monitor operational-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 adaptive security appliance, use the **show snmp-server engineid** command in privileged EXEC mode.

show snmp-server engineid

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	8.2(1)	This command was introduced.

Examples The following is sample output from the **show snmp-server engineid** command:

```
hostname# 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 adaptive security appliance context. The engine ID is not configurable on the adaptive security appliance. 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.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	8.2(1)	This command was introduced.

Examples The following is sample output from the **show snmp-server group** command:

```
hostname# 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.
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.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.0(1)	This command was introduced.

Examples The following is sample output from the **show snmp-server statistics** command:

```
hostname# 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.
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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.2(1)	This command was introduced.

Examples

The following is sample output from the **show snmp-server user** command:

```
hostname# 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 adaptive security appliance.
- The storage-type, which indicates whether or not the settings have been set in volatile or temporary memory on the adaptive security appliance, or in nonvolatile or persistent memory, in which settings remain after the adaptive security appliance 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 ssh sessions

To display information about the active SSH session on the adaptive security appliance, use the **show ssh sessions** command in privileged EXEC mode.

```
show ssh sessions [ip_address]
```

Syntax Description	<i>ip_address</i>	(Optional) Displays session information for only the specified IP address.
---------------------------	-------------------	--

Defaults	No default behavior or values.
-----------------	--------------------------------

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

Usage Guidelines	<p>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 adaptive security appliance. 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.</p>
-------------------------	---

Examples	The following example demonstrates the output of the show ssh sessions command:
-----------------	--

```
hostname# 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
```

Related Commands

Command	Description
ssh disconnect	Disconnects an active SSH session.
ssh timeout	Sets the timeout value for idle SSH sessions.

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 adaptive security appliance loaded the startup configuration.
---------------------------	---------------	--

Defaults No default behavior or values.

Command Modes The 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	•	•	•	•	•

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)	Support for password encryption was added.

Usage Guidelines In multiple context mode, this command shows the startup configuration for your current execution space: the system configuration or the security context.

To clear the startup errors from memory, use the **clear startup-config errors** command.

The **show startup-config** command output displays encrypted, masked, or clear text passwords when password encryption is either enabled or disabled.

Examples The following is sample output from the **show startup-config** command:

```
hostname# 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 firewall11
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:

```

hostname# 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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

```
hostname# show sunrpc-server active
      LOCAL          FOREIGN          SERVICE TIMEOUT
-----
192.168.100.2/0 209.165.200.5/32780 100005 00:10:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the adaptive security appliance.
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

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **show switch mac-address-table** command in privileged EXEC mode to view the switch MAC address table.

show switch mac-address-table

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.2(1)	This command was introduced.

Usage Guidelines This command is for models with built-in switches only. 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.

```
hostname# 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 29-3 shows each field description:

Table 29-3 *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

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **show switch vlan** command in privileged EXEC mode to view the VLANs and the associated switch ports.

show switch vlan

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.2(1)	This command was introduced.

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.

```
hostname# 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 29-3 shows each field description:

Table 29-4 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 (-).

Table 29-4 *show switch vlan Fields*

Field	Description
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 tcpstat

To display the status of the adaptive security appliance TCP stack and the TCP connections that are terminated on the adaptive security appliance (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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the adaptive security appliance. The TCP statistics displayed are described in [Table 28](#).

Table 29-5 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.
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.

Table 29-5 TCP Statistics in the show tcpstat Command (continued)

Statistic	Description
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 adaptive security appliance:

```
hostname# 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** | **file** | **no-config**]

Syntax Description

detail	(Optional) Lists detailed information.
file	(Optional) Writes the output of the command to a file.
no-config	(Optional) Excludes the output of the running configuration.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The detail and file keywords were added.
7.2(1)	The output display was enhanced to display more detailed information about processes that hog the CPU.

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 display information that is used for technical support analysis, excluding the output of the running configuration:

```
hostname# show tech-support no-config

Cisco XXX Firewall Version X.X(X)
Cisco Device Manager Version X.X(X)

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

Hardware:   XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
```

```

BIOS Flash AT29C257 @ 0xffffd8000, 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 23:05:24.264 UTC Sat Nov 16 2002

----- show clock -----
00:08:14.911 UTC Sun Apr 17 2005

----- show memory -----
Free memory:             50708168 bytes
Used memory:            16400696 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 :           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	919

----- 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
    1267 packets input, 185042 bytes, 0 no buffer
    Received 1248 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    20 packets output, 1352 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 babbles, 0 late collisions, 9 deferred
    0 lost carrier, 0 no carrier
    input queue (curr/max blocks): hardware (13/128) 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 cpu hogging process -----
```

```
Process:      fover_parse, NUMHOG: 2, MAXHOG: 280, LASTHOG: 140
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           11a4d5
Traceback:    12135e 121893 121822 a10d8b 9fd061 114de6 113e56f
              777135 7a3858 7a3f59 700b7f 701fbf 14b984
```

```
----- show process -----
```

	PC	SP	STATE	Runtime	SBASE	Stack	Process
Hsi	001e3329	00763e7c	0053e5c8	0	00762ef4	3784/4096	arp_timer
Lsi	001e80e9	00807074	0053e5c8	0	008060fc	3832/4096	FragDBGc
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
Mwe	002e3a17	00c8f8d4	0053e5c8	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	XXX Garbage Collec
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	6952/8192	qos_metric_daemon
Mwe	00255a65	00dc9244	0053e5c8	0	00dc8adc	1436/2048	IP Background
Lwe	002e450e	00e7bb94	00552c30	0	00e7ad1c	3704/4096	XXX/trace
Lwe	002e471e	00e7cc44	00553368	0	00e7bdcc	3704/4096	XXX/tconsole
Hwe	001e5368	00e7ed44	00730674	0	00e7ce9c	7228/8192	XXX/intf0
Hwe	001e5368	00e80e14	007305d4	0	00e7ef6c	7228/8192	XXX/intf1
Hwe	001e5368	00e82ee4	00730534	2470	00e8103c	4892/8192	XXX/intf2
H*	0011d7f7	0009ff2c	0053e5b0	780	00e8511c	13004/16384	ci/console
Csi	002dd8ab	00e8a124	0053e5c8	0	00e891cc	3396/4096	update_cpu_usage
Hwe	002cb4d1	00f2bfb4	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
Crđ	001db37f	00f32084	0053ea40	121094970	00f310fc	3744/4096	557poll
Lsi	001db435	00f33124	0053e5c8	0	00f321ac	3700/4096	557timer
Hwe	001e5398	00f441dc	008121e0	0	00f43294	3912/4096	fover_ip0
Cwe	001dcdad	00f4523c	00872b48	20	00f44344	3528/4096	ip/0:0
Hwe	001e5398	00f4633c	008121bc	0	00f453f4	3532/4096	icmp0
Hwe	001e5398	00f47404	00812198	0	00f464cc	3896/4096	udp_thread/0
Hwe	001e5398	00f4849c	00812174	0	00f475a4	3832/4096	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	icmpl
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 205213.390 secs):
    1267 packets    185042 bytes
    0 pkts/sec      0 bytes/sec
  transmitted (in 205213.390 secs):
    20 packets      1352 bytes
    0 pkts/sec      0 bytes/sec

inside:
  received (in 205215.800 secs):
    0 packets       0 bytes
    0 pkts/sec      0 bytes/sec
  transmitted (in 205215.800 secs):
    1 packets       60 bytes
    0 pkts/sec      0 bytes/sec

intf2:
  received (in 205215.810 secs):
    0 packets       0 bytes
    0 pkts/sec      0 bytes/sec
  transmitted (in 205215.810 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
```

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 adaptive security appliance 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 adaptive security appliance
show processes	Displays a list of the processes that are running.
show running-config	Displays the configuration that is currently running on the adaptive security appliance.
show xlate	Displays information about the translation slot.

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 <i>min_display_rate</i>	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the <i>min_display_rate</i> 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 no data UDP session attack.

Defaults 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	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
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 adaptive security appliance computes the event counts 30 times over the average rate interval; in other words, the adaptive security appliance 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 adaptive security appliance 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:

```
hostname# 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 targetted host IP addresses.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
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.

Examples

The following is sample output from the **show threat-detection scanning-threat** command:

```
hostname# show threat-detection scanning-threat
Latest Target Host & Subnet List:
 192.168.1.0
 192.168.1.249
Latest Attacker Host & Subnet List:
 192.168.10.234
 192.168.10.0
 192.168.10.2
 192.168.10.3
 192.168.10.4
 192.168.10.5
 192.168.10.6
 192.168.10.7
 192.168.10.8
 192.168.10.9
```

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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
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

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:

```
hostname# show threat-detection shun
Shunned Host List:
10.1.1.6
198.1.6.7
```

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.
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	
<i>ip_address</i>	(Optional) Shows statistics for a particular host.
<i>mask</i>	(Optional) Sets the subnet mask for the host IP address.
min-display-rate <i>min_display_rate</i>	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the <i>min_display_rate</i> between 0 and 2147483647.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	8.0(2)	This command was introduced.
	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 adaptive security appliance computes the event counts 30 times over the average rate interval; in other words, the adaptive security appliance 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 adaptive security appliance 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:

```
hostname# 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 29-6 shows each field description.

Table 29-6 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.

Table 29-6 show threat-detection statistics host Fields (continued)

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 no data UDP 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 adaptive security appliance 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 adaptive security appliance 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.

Table 29-6 show threat-detection statistics host Fields (continued)

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	
<i>start_port</i> [- <i>end_port</i>]	(Optional) Shows statistics for a particular port or range of ports, between 0 and 65535.
min-display-rate <i>min_display_rate</i>	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the <i>min_display_rate</i> between 0 and 2147483647.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	8.0(2)	This command was introduced.
	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 adaptive security appliance computes the event counts 30 times over the average rate interval; in other words, the adaptive security appliance 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 adaptive security appliance 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:

```
hostname# 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 29-6 shows each field description.

Table 29-7 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 adaptive security appliance 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 adaptive security appliance 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.
<i>port_number/port_name</i>	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.

Table 29-7 *show threat-detection statistics port Fields (continued)*

Field	Description
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
<i>protocol_number</i>	(Optional) Shows statistics for a specific protocol number, between 0 and 255.
min-display-rate <i>min_display_rate</i>	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the <i>min_display_rate</i> between 0 and 2147483647.
<i>protocol_name</i>	(Optional) Shows statistics for a specific protocol name: <ul style="list-style-type: none"> • ah • eigrp • esp • gre • icmp • igmp • igrp • ip • ipinip • ipsec • nos • ospf • pcp • pim • pptp • snp • tcp • udp

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
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 adaptive security appliance computes the event counts 30 times over the average rate interval; in other words, the adaptive security appliance 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 adaptive security appliance 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:

```
hostname# 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 29-6 shows each field description.

Table 29-8 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 adaptive security appliance 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 adaptive security appliance 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.
<i>protocol_number/ protocol_name</i>	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.

Table 29-8 *show threat-detection statistics protocol Fields (continued)*

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 denials 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 <i>min_display_rate</i>	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the <i>min_display_rate</i> 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 adaptive security appliance 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 adaptive security appliance 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 adaptive security appliance shows only the 24 hour time interval.
tcp-intercept	Shows TCP Intercept statistics. The display includes the top 10 protected servers under attack.

Defaults

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	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.
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 adaptive security appliance computes the event counts 30 times over the average rate interval; in other words, the adaptive security appliance 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 adaptive security appliance 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:

```
hostname# 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 29-6 shows each field description.

Table 29-9 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 than 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 adaptive security appliance 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 denials 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 adaptive security appliance 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.
1-hour, 8-hour	Shows statistics for these fixed rate intervals.
<i>acl_name</i> / <i>line_number</i>	Shows the access list name and line number of the ACE that caused the denials.

The following is sample output from the **show threat-detection statistics top access-list rate-1** command:

```
hostname# 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:

```
hostname# 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 29-10 shows each field description.

Table 29-10 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 than 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 29-6.
Current(eps)	See the description in Table 29-6.

Table 29-10 show threat-detection statistics top port-protocol Fields (continued)

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	See the description in Table 29-6 .
<i>Time_interval</i> Sent byte	Shows the number of successful bytes sent from the listed ports and protocols for each time period.
<i>Time_interval</i> Sent packet	Shows the number of successful packets sent from the listed ports and protocols for each time period.
<i>Time_interval</i> 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.
<i>Time_interval</i> Recv byte	Shows the number of successful bytes received by the listed ports and protocols for each time period.
<i>Time_interval</i> Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
<i>Time_interval</i> 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.
<i>port_number/port_name</i>	Shows the port number and name where the packet or byte was sent, received, or dropped.
<i>protocol_number/protocol_name</i>	Shows the protocol number and name where the packet or byte was sent, received, or dropped.

The following is sample output from the **show threat-detection statistics top host** command:

```
hostname# 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 29-11 shows each field description.

Table 29-11 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 than 10 hosts might be listed.
Average(eps)	See the description in Table 29-6.
Current(eps)	See the description in Table 29-6.
Trigger	See the description in Table 29-6.
Total events	See the description in Table 29-6.
<i>Time_interval</i> Sent byte	Shows the number of successful bytes sent to the listed hosts for each time period.
<i>Time_interval</i> Sent packet	Shows the number of successful packets sent to the listed hosts for each time period.
<i>Time_interval</i> 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.
<i>Time_interval</i> Recv byte	Shows the number of successful bytes received by the listed hosts for each time period.
<i>Time_interval</i> Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
<i>Time_interval</i> 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.
<i>host_ip_address</i>	Shows the host IP address where the packet or byte was sent, received, or dropped.

The following is sample output from the **show threat-detection statistics top tcp-intercept** command:

```

hostname# 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)

```

show threat-detection statistics top

```

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)

```

Table 29-12 shows each field description.

Table 29-12 show threat-detection statistics top tcp-intercept Fields

Field	Description
Monitoring window size:	Shows the period of time over which the adaptive security appliance 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 adaptive security appliance samples data 30 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 30.
<i>rank</i>	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
<i>server_ip:port</i>	Shows the server IP address and the port on which it is being attacked.
<i>interface</i>	Shows the interface through which the server is being attacked.
<i>avg_rate</i>	Shows the average rate of attack, in attacks per second over the sampling period
<i>current_rate</i>	Shows the current attack rate, in attacks per second.
<i>total</i>	Shows the total number of attacks.
<i>attacker_ip</i>	Shows the attacker IP address.
<i>(last_attack_time ago)</i>	Shows when the last attack occurred.

The following is sample output from the **show threat-detection statistics top tcp-intercept long** command with the real source IP address in parentheses:

```

hostname# 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:

```

hostname# 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 29-13 shows each field description.

Table 29-13 show threat-detection statistics top tcp-intercept detail Fields

Field	Description
Monitoring window size:	Shows the period of time over which the adaptive security appliance 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 adaptive security appliance samples data 30 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 30.
<i>rank</i>	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
<i>server_ip:port</i>	Shows the server IP address and the port on which it is being attacked.
<i>interface</i>	Shows the interface through which the server is being attacked.
<i>avg_rate</i>	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 adaptive security appliance samples the data every 30 seconds over the rate interval.
<i>current_rate</i>	Shows the current attack rate, in attacks per second.
<i>total</i>	Shows the total number of attacks.
<i>attacker_ip or <various> Last: attacker_ip</i>	Shows the attacker IP address. If there is more than one attacker, then “<various>” displays followed by the last attacker IP address.
<i>(last_attack_time ago)</i>	Shows when the last attack occurred.
<i>sampling data</i>	Shows all 30 sampling data values, which show the number of attacks at each interval.

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.

Command	Description
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

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]]
```

Syntax Description

cert-dump	Dumps the local dynamic certificate. Output is a hex dump of the LDC.
count	Shows only the session counters.
detail	Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC.
host <i>host_addr</i>	Specifies a particular host to show the sessions associated with.
session	Shows active TLS proxy sessions.
<i>tls_name</i>	Name of the TLS proxy to show.

Defaults

No default behavior or values.

Command Modes

The following table 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	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Examples

The following is sample output from the **show tls-proxy** command:

```
hostname# 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:

```
hostname# 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:

```
hostname# 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:
```

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	Shows running configuration of all or specified TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show track

To display information about object tracked by the tracking process, use the **show track** command in user EXEC mode.

```
show track [track-id]
```

Syntax Description	<i>track-id</i>	A tracking entry object ID. Valid values are from 1 to 500.
---------------------------	-----------------	---

Defaults	If the <i>track-id</i> 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	•	—	•	—	—

Command History	Release	Modification
	7.2(1)	This command was introduced.

Examples	The following is sample output from the show track command:
-----------------	--

```
hostname(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.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	7.2(1)	Special display for the ASA 5550 adaptive security appliance was added.

Usage Guidelines The **show traffic** command lists the number of packets and bytes moving through through each interface since the last **show traffic** command was entered or since the adaptive adaptive security appliance came online. The number of seconds is the duration the adaptive adaptive security appliance 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 adaptive security appliance, the **show traffic** command also shows the aggregated throughput per slot. Because the ASA 5550 adaptive security appliance requires traffic to be evenly distributed across slots fro maximum throughput, this display helps you determine if the traffic is distributed evenly.

Examples The following example shows output from the **show traffic** command:

```
hostname# 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/sec

Ethernet0:
  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 adaptive security appliance, 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%|*****

```

Related Commands

Command	Description
clear traffic	Resets the counters for transmit and receive activity.

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.

Defaults

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	•	•	—	—	•

Command History

Release	Modification
Preexisting	This command was preexisting.

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 adaptive security appliance 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 whether 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:

```
hostname(config)# show uauth
                Current      Most Seen
Authenticated Users      0          0
Authen In Progress      0          1
```

This example shows sample output from the **show uauth** command when three users are authenticated and authorized to use services through the adaptive security appliance:

```
hostname(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	Remove current user authentication and authorization information.
timeout	Set 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.
--------------------	------------------	--

Defaults	No default behavior or values.
----------	--------------------------------

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

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:
----------	--

```
hostname# 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.

Examples	The following is sample output from the show url-block block statistics command:
----------	---

```
hostname# 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.

Defaults No default behavior or values.

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

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

Command History	Release	Modification
	Preexisting	This command was preexisting.

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 adaptive security appliance has looked for a cache entry.
- Hits—The number of times the adaptive security appliance 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:

```
hostname# 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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 n2h2 host 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:

```
hostname## 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
HTTPSs allowed by cache/server     70483/85165
HTTPSs 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.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

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

Syntax Description

This command has no arguments or keywords.

Defaults

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	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.
7.2(1)	In stateful failover mode, an additional line showing cluster uptime is displayed.

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 (R or UR), and time stamp for when the configuration was last modified.

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.

- If you downgrade to an earlier release, your key for the current release might allow for more security contexts than the earlier release supports. When the value of the security contexts in the key exceeds the platform limit, the following message appears in the show activation-key output:

```
The Running Activation Key feature: 50 security contexts exceeds the limit in the platform, reduce to 20 security contexts.
```

- If you downgrade to an earlier release, your key for the current release might enable GTP/GPRS even though it is not allowed in the earlier release. When the key enables GTP/GPRS but the software version does not allow it, the following message appears in the show activation-key output:

```
The Running Activation Key feature: GTP/GPRS is not allowed in the platform, disable GTP/GPRS.
```

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.

Examples

The following example shows how to display 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:

```
hostname# show version

Cisco Adaptive Security Appliance Software Version 8.0(0)
Device Manager Version 6.0(0)

Compiled on Mon 16-April-07 03:29 by root
System image file is "disk0:/cdisk.bin"
Config file at boot was "disk0:/main_backup.cfg"

hostname up 2 days 10 hours
failover cluster up 2 days 11 hours

Hardware:   ASA5520, 1024 MB RAM, CPU Pentium 4 Celeron 2000 MHz
BIOS Flash M50FW016 @ 0xffe00000, 2048KB

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-2.01
IPSec microcode    : CNLite-MC-IPSECm-MAIN-2.04
0: Ext: GigabitEthernet0/0 : address is 000b.fcf8.c44e, irq 9
1: Ext: GigabitEthernet0/1 : address is 000b.fcf8.c44f, irq 9
2: Ext: GigabitEthernet0/2 : address is 000b.fcf8.c450, irq 9
3: Ext: GigabitEthernet0/3 : address is 000b.fcf8.c451, irq 9
4: Ext: Management0/0      : address is 000b.fcf8.c44d, irq 11
5: Int: Not used           : irq 11
6: Int: Not used           : irq 5

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs               : 150
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Security Contexts           : 10
GTP/GPRS                    : Enabled
VPN Peers                   : 750
WebVPN Peers                : 500
Advanced Endpoint Assessment : Disabled

This platform has an ASA 5520 VPN Plus license.

Serial Number: P3000000098
Running Activation Key: 0x7c2e394b 0x0c842e53 0x98f3edf0 0x8c1888b0 0x0336f1ac
Configuration register is 0x1
Configuration last modified by enable_15 at 14:17:59.410 EST Wed April 16 2007
hostname#
```

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.
```

Related Commands

Command	Description
eject	Allows shutdown of external compact Flash device before physical removal from the security appliance.
show hardware	Displays detail hardware information.
show serial	Displays the hardware serial information.
show uptime	Displays how long the adaptive security appliance has been up.

show vlan

To display all VLANs configured on the adaptive security appliance, use the **show vlan** command in privileged EXEC mode.

show vlan

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example displays the configured VLANs:

```
hostname# show vlan
10-11, 30, 40, 300
```

Related Commands

Command	Description
clear interface	Clears counters for the show interface command.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.

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.

Defaults

No default behavior or values.

Command Modes

The 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	•	—	•	—	—
Privileged EXEC	•	—	•	—	—
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	Added separate IPSec and SSL columns for both Load (%) display and Session display in the output example.

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 adaptive security appliance 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:

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
```

show vpn load-balancing

```

Public IP          Role  Pri   Model          Load (%)          Sessions
                  IPsec SSL          IPsec  SSL
-----
* 192.168.1.40    Master 10    PIX-515         0      0           0      0
  192.168.1.110  Backup 5    PIX-515         0      0           0      0
hostname(config-load-balancing)#

```

If the local device is not participating in the VPN load-balancing cluster, the **show vpn load-balancing** command shows a different result:

```

hostname(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 [detail] [full] {remote | l2l | index indexnumber | webvpn | email-proxy | svc}
[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 Descriptions

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 adaptive security appliance displays the detailed output in a machine-readable format.
filter <i>filter_criteria</i>	(Optional) Filters the output to display only the information you specify by using one or more of the filter options. For a list of <i>filter_criteria</i> options, see the “Usage Guidelines” section.
full	(Optional) Displays streamed, untruncated output. Output is delineated by characters and a string between records.
<i>session_type</i>	(Optional) To show data for a specific session type, enter one of the following keywords: <ul style="list-style-type: none"> • email-proxy—Displays email-proxy sessions. • index <i>indexnumber</i>—Displays a single session by index number. Specify the index number for the session, 1 - 750. • l2l—Displays VPN LAN-to-LAN session information. • ratio—Displays VPN Session protocol or encryption ratios. • remote—Displays IPsec remote access sessions. • summary—Displays the VPN session summary. • svc—Displays SSL VPN Client sessions. • vpn-lb—Displays VPN Load Balancing management sessions. • webvpn—Displays information about clientless SSL VPN sessions.
sort <i>sort_criteria</i>	(Optional) Sorts the output according to the sort option you specify. For a list of <i>sort_criteria</i> options, see the “Usage Guidelines” section.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.
8.0(2)	Added VLAN field description.
8.0(5)	Added inactive as a filter option and inactivity as a sort option.
8.2(1)	License information was added to the output.

Usage Guidelines

You can use the following options to filter and to sort the session display:

Filter/Sort Option	Description
filter a-ipaddress <i>IPaddr</i>	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 encryption <i>encryption-algo</i>	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 lost connectivity. Each session is time stamped with the SSL tunnel drop time. If the session is active, 00:00m:00s is displayed..
sort inactivity	Sorts inactive sessions.
filter ipaddress <i>IPaddr</i>	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 name <i>username</i>	Filters the output to display sessions for the specified username(s).
sort name	Sorts the display by usernames in alphabetical order.
filter p-address <i>IPaddr</i>	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 protocol <i>protocol-name</i>	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/Sort Option	Description
filter tunnel-group <i>groupname</i>	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}

Examples

The following is sample output from the **show vpn-sessiondb** command:

```

hostname# show vpn-sessiondb
Active Session Summary

Sessions:
              Active : Cumulative : Peak Concurrent
SSL VPN      :          0 :          0 :
  Clientless only :          0 :          0 :
  With client   :          0 :          0 :
Email Proxy   :          0 :          0 :
IPsec LAN-to-LAN :          0 :          0 :
IPsec Remote Access :          0 :          0 :
VPN Load Balancing :          0 :          0 :
Totals       :          0 :          0

License Information:
Multi-site VPN License Information:
  SSL VPN      :          10000
  Allocated to this device :          0
  Allocated in network    :          0
  Device limit           :          250

IPsec :    250   Configured :    250   Active :    0   Load : 0%
SSL VPN :    10   Configured :    10   Active :    0   Load : 0%
              Active : Cumulative : Peak Concurrent
IPsec      :          0 :          0 :          0
SSL VPN    :          0 :          0 :          0
  AnyConnect Mobile :          0 :          0 :          0
  Linksys Phone   :          0 :          0 :          0
Totals      :          0 :          0 :          0

Tunnels:
  No tunnels to display

Active NAC Sessions:
  No NAC sessions to display

Active VLAN Mapping Sessions:
  No VLAN Mapping sessions to display

```

The following is sample output from the **show vpn-sessiondb detail 121** command, showing detailed information about LAN-to-LAN sessions:

```

hostname# show vpn-sessiondb detail 121
Session Type: LAN-to-LAN Detailed
Connection : 172.16.0.1
Index      : 1
Protocol   : IPSecLAN2LAN
Bytes Tx   : 48484156
Login Time : 09:32:03 est Mon Aug 2 2004
Duration   : 6:16:26
IP Addr    : 172.16.0.1
Encryption : AES256
Bytes Rx   : 875049248

```

```

Filter Name :

IKE Sessions: 1 IPSec Sessions: 2

IKE:
  Session ID      : 1
  UDP Src Port    : 500
  IKE Neg Mode    : Main
  Encryption      : AES256
  Rekey Int (T)  : 86400 Seconds
  D/H Group      : 5
  UDP Dst Port    : 500
  Auth Mode      : preSharedKeys
  Hashing        : SHA1
  Rekey Left(T)  : 63814 Seconds

IPSec:
  Session ID      : 2
  Local Addr     : 10.0.0.0/255.255.255.0
  Remote Addr    : 209.165.201.30/255.255.255.0
  Encryption      : AES256
  Encapsulation  : Tunnel
  Rekey Int (T)  : 28800 Seconds
  Bytes Tx       : 46865224
  Pkts Tx        : 1635314
  Hashing        : SHA1
  PFS Group      : 5
  Rekey Left(T)  : 10903 Seconds
  Bytes Rx       : 2639672
  Pkts Rx        : 37526

IPSec:
  Session ID      : 3
  Local Addr     : 10.0.0.1/255.255.255.0
  Remote Addr    : 209.165.201.30/255.255.255.0
  Encryption      : AES256
  Encapsulation  : Tunnel
  Rekey Int (T)  : 28800 Seconds
  Bytes Tx       : 1619268
  Pkts Tx        : 19277
  Hashing        : SHA1
  PFS Group      : 5
  Rekey Left(T)  : 6282 Seconds
  Bytes Rx       : 872409912
  Pkts Rx        : 1596809

```

hostname#

The following is sample output from the **show vpn-sessiondb detail full index 4** command, showing the details of single session:

```

AsaNacDev# show vpn-sessiondb detail full index 4
Session Type: Remote Detailed |

Index: 2 | EasyVPN: 0 | Username: uuuu | Group: DfltGrpPolicy | Tunnel Group:
regr3000multigroup | IP Addr: 192.168.2.80 | Public IP: 10.44.173.216 | Protocol:
IPSecOverUDP | Encryption: 3DES | Login Time: 12:51:54 EDT Wed Jun 21 2006 |Duration:
0h:02m:44s | Bytes Tx: 2134 | Bytes Rx: 8535 | Client Type: WinNT | Client Ver: 4.0.5
(Rel) | Filter Name: | NAC Result: N/A | Posture Token: : | VM Result: Static | VLAN: 10
||

IKE Sessions: 1
| IPSecOverUDP Sessions: 1
|

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeys | UDP Source Port: 500 |
UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES | Hashing:
SHA1 | Diffie-Hellman Group: 2 | Rekey Time Interval: 40000 Seconds| Rekey Left(T): 39836
Seconds ||

Type: IPSecOverUDP | Session ID: 2 | Local IP Addr: 0.0.0.0/0.0.0.0/0/0 | Remote IP Addr:
192.168.2.80/255.255.255.255/0/0 | Encryption: 3DES | Hashing: SHA1 | Encapsulation:
Tunnel | UDP Destination Port: 10000 | Rekey Time Interval: 28800 Seconds | Rekey Left(T):
28636 Seconds | Idle Time Out: 30 Minutes | Idle TO Left: 30 Minutes | Bytes Tx: 2134 |
Bytes Rx: 8535 | Packets Tx: 15 | Packets Rx: 2134 | ||

```

```

VLAN Mapping: VLAN: 10 |

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  : bxbvplab
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

```

As shown in the examples, the fields displayed in response to the **show vpn-sessiondb** command vary, depending on the keywords you enter. [Table 29-14](#) explains these fields.

Table 29-14 show vpn-sessiondb Command Fields

Field	Description
Auth Mode	Protocol or mode used to authenticate this session.
Bytes Rx	Total number of bytes received from the remote peer or client by the adaptive security appliance.
Bytes Tx	Number of bytes transmitted to the remote peer or client by the adaptive security appliance.

Table 29-14 show vpn-sessiondb Command Fields (continued)

Field	Description
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.
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.
Encryption	Data encryption algorithm this session is using.
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 adaptive security appliance).
Login Time	Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.

Table 29-14 show vpn-sessiondb Command Fields (continued)

Field	Description
NAC Result	<p>State of Network Admission Control Posture Validation. It can be one of the following:</p> <ul style="list-style-type: none"> 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 adaptive security appliance. Non-Responsive—The remote host did not respond to the EAPoUDP Hello message. Hold-off—The adaptive security appliance 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 adaptive security appliance.
Packets Tx	Number of packets transmitted to the remote peer by the adaptive security appliance.
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 adaptive security appliance 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	<p>Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the adaptive security appliance. The Redirect URL is an optional part of the access policy payload. The adaptive security appliance 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 adaptive security appliance does not redirect HTTP and HTTPS requests from the remote host.</p> <p>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.</p>
Rekey Int (T)	Lifetime of the IPsec (IKE) SA encryption keys.
Rekey Left (T)	Lifetime remaining of the IPsec (IKE) SA encryption keys.
Rekey Time Interval	Lifetime of the IPsec (IKE) SA encryption keys.

Table 29-14 show vpn-sessiondb Command Fields (continued)

Field	Description
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 adaptive security appliance 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 adaptive security appliance 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 adaptive security appliance for UDP.
Username	User login name with which the session is established.
VLAN	Egress VLAN interface assigned to this session. The adaptive security appliance forwards all traffic to that VLAN. One of the following elements specifies the value: <ul style="list-style-type: none"> • Group policy • Inherited group policy

Related Commands

Command	Description
show running-configuration vpn-sessiondb	Displays the VPN session database running configuration.
show vpn-sessiondb ratio	Displays VPN session encryption or protocol ratios.
show vpn-sessiondb summary	Displays a summary of all VPN sessions.

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 <i>groupname</i>	Filters the output to include session ratios only for the tunnel group you specify.
protocol	Identifies the protocols you want to display. Protocols include: IKE SMTPS IMAP4S userHTTPS IPSec vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb ratio** command, with **encryption** as the argument:

```
hostname# show vpn-sessiondb ratio enc
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:

```
hostname# 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 Commandss

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 AnyConnect, and NAC sessions, use the **show vpn-sessiondb summary** command in privileged EXEC mode.

show vpn-sessiondb summary

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(5)	Added new output for active, cumulative, peak concurrent, and inactive.
8.0(2)	Added the VLAN Mapping Sessions table.
7.0(7)	This command was introduced.

Examples

The following is sample output for the **show vpn-sessiondb summary** command on an active device:



Note A device in standby does not differentiate active from inactive sessions.

```

hostname# show vpn-sessiondb summary
Active Session Summary

Sessions:
              Active : Cumulative : Peak Concurrent
      Active :Cumulative :Peak Concurrent :Inactive :
SSL VPN   :      0 :      1 :      1 :
  Clientless only  0 :      1 :      1 :
  With client    0 :      0 :      0 :      0
Totals      0 :      1 :

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 :
Tunnels:
                Active : Cumulative : Peak Concurrent
Clientless     :          3 :        100 :          5
SSL-Tunnel     :          2 :        156 :          5
DTLS-Tunnel    :          2 :        119 :          4
Totals        :          7 :        375 :
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

```

F1-asal#

A session is a VPN tunnel established with a specific peer. 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.

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 inactive sessions. These are AnyConnect sessions without an active SSL tunnel associated with them.

Table 29-15 explains the fields in the Active Sessions and Session Information tables.

Table 29-15 *show vpn-sessiondb summary Command: Active Sessions and Session Information Fields*

Field	Description
Concurrent Limit	Maximum number of concurrently active sessions permitted on this adaptive security appliance.
Cumulative Sessions	Number of sessions of all types since the adaptive security appliance 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 active since the adaptive security appliance was last booted or reset.

Table 29-15 *show vpn-sessiondb summary Command: Active Sessions and Session Information Fields*

Field	Description
Percent Session Load	Percentage 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: <ul style="list-style-type: none"> • Maximum number of IPsec and SSL VPN sessions licensed. • Maximum number of sessions configured using the following commands: <ul style="list-style-type: none"> – vpn-sessiondb max-session-limit – vpn-sessiondb max-webvpn-session-limit
Remote Access	Number of PPTP, L2TP, 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.

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 29-14](#) explains the fields in the Active NAC Sessions and Total Cumulative NAC Sessions tables.

Table 29-16 *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 adaptive security appliance.
Hold-off	Number of peers for which the adaptive security appliance 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.
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 adaptive security appliance configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the adaptive security appliance for these peers. Otherwise, the adaptive security appliance 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 29-17 explains the fields in the Active VLAN Mapping Sessions and Cumulative VLAN Mapping Sessions tables.

Table 29-17 *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

web-cache	Specifies statistics for the web-cache service.
<i>service-number</i>	(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.
<i>detail</i>	(Optional) Displays information about the router and all web caches.
<i>view</i>	(Optional) Displays other members of a particular service group have or have not been detected.

Defaults

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	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to display WCCP information:

```
hostname(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
hostname(config)#
```

Related Commands

Commands	Description
wccp	Enables support of WCCP with service groups.
wccp redirect	Enables support of WCCP redirection.

show webvpn csd

To determine whether CSD is enabled and, if so, display the CSD version in the running configuration, or 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 securedesktop_asa_<n>_<n>*.pkg.
--------------------	----------	--

Defaults No default behavior or values.

Command Modes The following table 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	•	—	•	—	—

Command History	Release	Modification
	7.1(1)	This command was introduced.

Usage Guidelines Use the **show webvpn csd** command to check the operational status of CSD. The CLI responds with one of the following messages when you enter this command:

- Secure Desktop is not enabled.
CSD is in the running configuration, but it is disabled. Go to webvpn configuration mode and enter the **csd enable** command to enable CSD.
- Secure Desktop version *n.n.n.n* is currently installed and enabled.
CSD is enabled. The distribution package read from the flash device determines the version number. You can access Cisco Secure Desktop Manager through the ASDM Configuration > CSD menu path. CSD is accessible to users only if the CSD configuration contains a location.

Use the **show webvpn csd image** command to test a file to see if it is a valid CSD distribution package. Similarly, the **csd image** command, when entered in webvpn configuration mode, installs CSD only if the file you name in the command is a valid CSD distribution package. Otherwise, it displays an “ERROR: Unable to use CSD image” message.

The **show webvpn csd image** command tests a file to see if it is a valid CSD distribution package without installing CSD automatically if the file is valid. 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 `securedesktop_asa_<n>_<n>*.pkg`. If it is, replace the file with a fresh one obtained from the following website:
<http://www.cisco.com/cisco/software/navigator.html>
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 : 3.1.0.25
Built on : Wed 10/19/2005 14:51:23.82
Note that the CLI provides both the version and date stamp if the file is valid.

Examples

The following example indicates CSD is installed in the running configuration and enabled:

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname#
```

The following example shows the file specified is a valid CSD image:

```
hostname#show webvpn csd image securedesktop_asa_3_1_0_25.pkg

This is a valid Cisco Secure Desktop image:
  Version   : 3.1.0.25
  Built on  : Wed 10/19/2005 14:51:23.82

hostname#
```

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 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	<i>tunnel-group</i>	(Optional) Specifies a particular tunnel group for which to show the group aliases.
---------------------------	---------------------	---

Defaults 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	•	—	•	—	—

Command History	Release	Modification
	7.1	This command was introduced.

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:

```
hostname# show webvpn group-alias devtest
QA
Fra-QA
```

Related Commands	Command	Description
	group-alias	Specifies one or more URLs for the group.
	tunnel-group	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.
	webvpn-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	<i>tunnel-group</i> (Optional) Specifies a particular tunnel group for which to show the URLs.
---------------------------	--

Defaults	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	•	—	•	—	—

Command History	Release	Modification
	7.1(1)	This command was introduced.

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:
-----------------	---

```
hostname# show webvpn group-url
http://www.cisco.com
https://fra1.vpn.com
https://fra2.vpn.com
```

Related Commands	Command	Description
	group-url	Specifies one or more URLs for the group.
	tunnel-group	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.
	webvpn-attributes	

show webvpn sso-server

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

<i>name</i>	Optionally specifies the name of the SSO server. The server name must be between four and 31 characters in length.
-------------	--

Defaults

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	•	—	•	—	—
config-webvpn-sso-siteminder	•	—	•	—	—
Privileged EXEC	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

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:

```
hostname# 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
hostname#

```

The following example of the command issued without a specific SSO server name, displays statistics for all configured SSO servers on the adaptive security appliance:

```

hostname#(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
asal(config-webvpn)#

```

Related Commands	Command	Description
	max-retry-attempts	Configures the number of times the adaptive security appliance 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.
	sso-server	Creates a single sign-on server.
	web-agent-url	Specifies the SSO server URL to which the adaptive security appliance makes SiteMinder SSO authentication requests.

show webvpn svc

To view information about SSL VPN client images installed on the adaptive security appliance and loaded in cache memory, or to test a file to see if it is a valid client image, use the **show webvpn svc** command from privileged EXEC mode.

```
show webvpn svc [image filename]
```

Syntax Description

image filename Specifies the name of a file to test as an SSL VPN client image file.

Defaults

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	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Use the **show webvpn svc** 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 svc** command for currently installed images:

```
hostname# show webvpn svc
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 svc image filename** command for a valid image:

```
F1(config-webvpn)# show webvpn svc 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
svc enable	Enables the adaptive security appliance to download the SSL VPN client to remote PCs.
svc 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 xlate

To display information about the translation slots, 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] [state state] [debug] [detail]
```

show xlate count

Syntax Description

count	Displays the translation count.
debug	(Optional) Displays xlate debug information.
detail	(Optional) Displays detail xlate information.
global ip1[-ip2]	(Optional) Displays the active translations by global IP address or range of addresses.
gport port1[-port2]	Displays the active translations by the global port or range of ports.
interface if_name	(Optional) Displays the active translations by interface.
local ip1[-ip2]	(Optional) Displays the active translations by local IP address or range of addresses.
lport port1[-port2]	Displays the active translations by local port or range of ports.
netmask mask	(Optional) Specifies the network mask to qualify the global or local IP addresses.
state state	(Optional) Displays the active translations by state. You can enter one or more of the following states: <ul style="list-style-type: none"> • static—specifies static translations. • portmap—specifies PAT global translations. • norandomseq—specifies a nat or static translation with the norandomseq setting. • identity—specifies nat 0 identity address translations. When specifying more than one state, separate the states with a space.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **show xlate** command displays the contents of the translation slots. The **show xlate detail** command displays the following information:

- **{ICMP|TCP|UDP} PAT from** *interface:real-address/real-port to interface:mapped-address/mapped-port* **flags translation-flags**
- **NAT from** *interface:real-address/real-port to interface:mapped-address/mapped-port* **flags translation-flags**

The translation flags are defined in [Table 29-18](#).

Table 29-18 Translation Flags

Flag	Description
s	Static translation slot
d	Dump translation slot on next cleaning cycle
r	Port map translation (Port Address Translation)
n	No randomization of TCP sequence number
i	Inside address translation
D	DNS A RR rewrite
I	Identity translation from nat 0

**Note**

When the **vpncient** configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

Examples

The following is sample output from the **show xlate** command. It shows how translation slot information with three active PATs.

```
hostname# show xlate
3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

The following is sample output from the **show xlate detail** command. It shows the translation type and interface information with three active PATs.

The first entry is a TCP PAT for host port (10.1.1.15, 1025) on the inside network to host-port (192.150.49.1, 1024) on the outside network. The **r** flag indicates that the translation is a PAT. The **i** flag indicates that the translation applies to the inside address port.

The second entry is a UDP PAT for host port (10.1.1.15, 1028) on the inside network to host port (192.150.49.1, 1024) on the outside network. The **r** flag indicates that the translation is a PAT. The **i** flag indicates that the translation applies to the inside address port.

The third entry is an ICMP PAT for host-ICMP-id (10.1.1.15, 21505) on the inside network to host-ICMP-id (192.150.49.1, 0) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address ICMP ID.

The inside address fields appear as source addresses on packets traversing from the more secure interface to the less secure interface. They appear as destination addresses on packets traversing from the less secure interface to the more secure interface.

```
hostname# show xlate detail
```

```
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
```

The following is sample output from the **show xlate** command. It shows two static translations. The first translation has one associated connection (called “nconns”), and the second translation has four associated connections.

```
hostname# show xlate
Global 209.165.201.10 Local 209.165.201.10 static nconns 1 econns 0
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
```

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.

