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.
dest_ip dest_mask	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 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 *protocol* 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.
icmp_control_message	(Optional) Specifies an ICMP control message of the traffic flow. Valid values for the *icmp_control_message* argument are listed in the "Usage Guidelines" section, below.
icmp_number	(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 *intf* argument, where *intf* 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.
src_ip src_mask	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)	The **shape** keyword was added.

Usage Guidelines The **flow** keyword lets you determine, for any flow that you can describe, the policies that the 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: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

The following is sample output from the **show service-policy inspect http** command. This example shows the statistics of each match command in a match-any class map.

```
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	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:

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines During FTP inspection, the security appliance can drop packets silently. To see whether the 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 security appliance infrequently drops packets silently; therefore, the output of this command rarely displays drop counters.

Table 1-1 describes the output from the **show service-policy inspect ftp** command:

Table 1-1   *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 security appliance attempts to allocate a data structure for a CP connection and the attempt fails. Check for low system memory.

Table 1-1   *FTP Drop Counter Descriptions*

Drop Counter	Counter increments...
Can't alloc FTP data structure drop	When the 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 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 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 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 security appliance expects to receive a PORT command but receives another command.
Cmd not supported drop	When the 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 security appliance receives a reply when a reply is not expected.
Retx cmd in cmd mode drop	When a retransmitted command is received in CMD mode.

Table 1-1   FTP Drop Counter Descriptions

Drop Counter	Counter increments...
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.
ap_name	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.
IMSI_value	Hexadecimal value that identifies the specific IMSI for which statistics are displayed.
interface	(Optional) Identifies a specific interface.
int	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.
IP_address	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.
tunnel_ID	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.
version_num	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		
				Multiple	
	Routed	Transparent	Single	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_pdpmcb | 0 | total deleted_pdpmcb | 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 1-2 describes each column the output from the **show service-policy inspect gtp pdp-context** command.

Table 1-2   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
class-map	Defines the traffic class to which to apply security actions.
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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 shun

To display shun information, use the **show shun** command in privileged EXEC mode.

show shun [*src_ip* | *statistics*]

Syntax Description

src_ip	(Optional) Displays the information for that address.
statistics	(Optional) Displays the interface counters only.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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:

| | Firewall Mode | | Security Context | | |
| | | | | Multiple | |
Command Mode	**Routed**	**Transparent**	**Single**	**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 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 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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

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, statistics for all SLA operations are displayed.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0        RTTMin: 0        RTTMax: 0
```

```
NumOfRTT: 0      RTTSum: 0        RTTSum2: 0
```

	Command	Description
Related Commands	**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 statistics

To display information about the 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   This command has no default settings.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples   This example shows how to display the SNMP server statistics:

```
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

Cisco Security Appliance Command Reference 7.2(2)

Command	Description
snmp-server	Provides the security appliance event information through SNMP.
clear configure snmp-server	Disables the Simple Network Management Protocol (SNMP) server.
show running-config snmp-server	Displays the SNMP server configuration.

show ssh sessions

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

> **show ssh sessions** [*ip_address*]

Syntax Description

ip_address	(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		
				Multiple	
	Routed	Transparent	Single	Context	System
Privileged EXEC	●	●	●	●	—

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The SID is a unique number that identifies the SSH session. The Client IP is the IP address of the system running an SSH client. The Version is the protocol version number that the SSH client supports. If the SSH only supports SSH version 1, then the Version column displays 1.5. If the SSH client supports both SSH version 1 and SSH version 2, then the Version column displays 1.99. If the SSH client only supports SSH version 2, then the Version column displays 2.0. The Encryption column shows the type of encryption that the SSH client is using. The State column shows the progress that the client is making as it interacts with the security appliance. The Username column lists the login username that has been authenticated for the session.

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 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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.

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.

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 7.0(0)28
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
```

```
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
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:

| | Firewall Mode | | Security Context | | |
| | | | | Multiple | |
Command Mode	Routed	Transparent	Single	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 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 1-3 shows each field description:

Table 1-3   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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 1-3 shows each field description:

Table 1-4   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 1-4   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 security appliance TCP stack and the TCP connections that are terminated on the 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 security appliance. The TCP statistics displayed are described in Table 28.

Table 1-5   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 1-5   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 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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-suppor**t 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
```

Cisco Security Appliance Command Reference 7.2(2)

```
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 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 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 Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 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 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  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 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

----------------- show failover ------------------


No license for Failover

----------------- show traffic ------------------


outside:
        received (in 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 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.
show perfmon	Displays information about the performance of the 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 security appliance.
show xlate	Displays information about the translation slot.

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

track-id	A tracking entry object ID. Valid values are from 1 to 500.

Defaults   If the *track-id* is not provided, then information about all tracking objects is displayed.

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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:

| | Firewall Mode | | Security Context | | |
| | | | | Multiple | |
Command Mode	Routed	Transparent	Single	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 security appliance came online. The number of seconds is the duration the 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 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 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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.

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 security appliance has looked for a cache entry.
- Hits—The number of times the 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
HTTPs allowed by cache/server    70483/85165
HTTPs denied by cache/server     801920/36819
FTPs total/allowed/denied        994387/155648/838739
FTPs allowed by cache/server     70483/85165
```

```
FTPs denied by cache/server     801920/36819
Requests dropped                28715
Server timeouts/retries         567/1350
Processed rate average 60s/300s 1524/1344 requests/second
Denied rate average 60s/300s    35648/33022 requests/second
Dropped rate average 60s/300s   156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                     UP
Vendor                          websense
Port                            17035
Requests total/allowed/denied   366519/255495/110457
Server timeouts/retries         567/1350
Responses received              365952
Response time average 60s/300s  2/1 seconds/request
192.168.0.2                      DOWN
Vendor                          websense
Port                            17035
Requests total/allowed/denied   0/0/0
Server timeouts/retries         0/0
Responses received              0
Response time average 60s/300s  0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message               Sent     Received
STATUS_REQUEST        411      0
LOOKUP_REQUEST        366519   365952
LOG_REQUEST           0        NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a global
and per-server basis.  The output is reformatted to provide: more-detailed information and
per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
url-block	Manage the URL buffers used for web server responses.

url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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.

Note   The uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value will continue to increase as long as the other unit continues to operate.

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 PIX Security Appliance Software Version 7.0(4)
Device Manager Version 5.0(4)

Compiled on Tue 27-Sep-05 10:41 by root
System image file is "flash:/cdisk.bin"
Config file at boot was "startup-config"

pix2 up 7 days 7 hours
failover cluster up 2 mins 44 secs


Hardware:   PIX-515E, 128 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

 0: Ext: Ethernet0          : address is 0011.2094.1d2b, irq 10
 1: Ext: Ethernet1          : address is 0011.2094.1d2c, irq 11

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Enabled
VPN Peers                   : Unlimited

This platform has an Unrestricted (UR) license.

Serial Number: 808184143
Running Activation Key: 0xcf22f25d 0xec1c3174 0x8cb138a0 0xaad8b878 0x4f32fd90
Configuration last modified by enable_15 at 14:18:26.103 UTC Thu Oct 6 2005
hostname#
```

Related Commands	Command	Description
	show hardware	Displays detail hardware information.
	show serial	Displays the hardware serial information.
	show uptime	Displays how long the security appliance has been up.

show vlan

To display all VLANs configured on the 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 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
```

```
                                      Load (%)          Sessions
Public IP       Role  Pri   Model     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.

```
                                      Load (%)          Sessions
Public IP       Role  Pri   Model     IPSec  SSL        IPSec  SSL
```

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}
    [filter {name *username* | ipaddress *IPaddr* | a-ipaddress *IPaddr* | p-ipaddress *IPaddr* |
    tunnel-group *groupname* | protocol *protocol-name* | encryption *encryption-algo*}]
    [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption}]

Syntax Descriptions

Granularity of Display	
detail	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 security appliance displays the detailed output in a machine-readable format.
filter	Filters the output to display only the information you specify by using one or more of the filter options. For more information, see usage notes.
full	Displays streamed, untruncated output. Output is delineated by	characters and a || string between records.
sort	Sorts the output according to the sort option you specify. For more information, see usage notes.
Session Type to Display	
email-proxy	Displays email-proxy sessions. You can display this information for e-mail proxy sessions, or you can filter it by using the following filter and sort options: **name** (connection name), **ipaddress** (client), **encryption**.
index *indexnumber*	Displays a single session by index number. Specify the index number for the session, 1 - 750. Filter and sort options do not apply.
l2l	Displays VPN LAN-to-LAN session information. You can display this information for all groups or you can filter it by using the following filter and sort options: **name**, **ipaddress**, **protocol, encryption**.
remote	Displays remote-access sessions. You can display this information for all groups or you can filter it by using the following filter options: **name**, **a-ipaddress**, **p-ipaddress, tunnel-group**, **protocol**, **encryption**.
webvpn	Displays information about WebVPN sessions. You can display this information for all groups or you can filter it by using the following filter and sort options: **name**, **ipaddress**, **encryption**.

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

Filter/Sort Option	Meaning
filter a-ipaddress *IPaddr*	Filters the output to display information for the specified assigned IP address or addresses only.
sort a-ipaddress	Sorts the display by assigned IP addresses.
filter encryption *encryption-algo*	Filters the output to display information for sessions using the specified encryption algorithm(s) only.
sort encryption	Sorts the display by encryption algorithm. Encryption algorithms include: aes128, aes192, aes256, des, 3des, rc4
filter ipaddress *IPaddr*	Filters the output to display information for the specified inside IP address or addresses only.
sort ipaddress	Sorts the display by inside IP addresses.
filter name *username*	Filters the output to display sessions for the specified username(s).
sort name	Sorts the display by usernames in alphabetical order.
filter p-address *IPaddr*	Filters the output to display information for the specified outside IP address only.
sort p-address	Sorts the display by the specified outside IP address or addresses.
filter protocol *protocol-name*	Filters the output to display information for sessions using the specified protocol(s) only.
sort protocol	Sorts the display by protocol. Protocols include: IKE, IMAP4S, IPSec, IPSecLAN2LAN, IPSecLAN2LANOverNatT, IPSecOverNatT, IPSecoverTCP, IPSecOverUDP, SMTPS, userHTTPS, vcaLAN2LAN
filter tunnel-group *groupname*	Filters the output to display information for the specified tunnel group(s) only.
sort tunnel-group	Sorts the display by tunnel group.
| character	Modifies the output, using the following arguments: {begin | include | exclude | grep | [-v]} {reg_exp}
<cr>	Sends the output to the console.

The following example, entered in privileged EXEC mode, shows detailed information about
LAN-to-LAN sessions:

```
hostname# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection  : 172.16.0.1
Index       : 1                      IP Addr      : 172.16.0.1
Protocol    : IPSecLAN2LAN           Encryption   : AES256
Bytes Tx    : 48484156               Bytes Rx     : 875049248
Login Time  : 09:32:03 est Mon Aug 2 2004
Duration    : 6:16:26
Filter Name :

IKE Sessions: 1 IPSec Sessions: 2

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

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              Hashing      : SHA1
  Encapsulation: Tunnel              PFS Group    : 5
  Rekey Int (T): 28800 Seconds       Rekey Left(T): 10903 Seconds
  Bytes Tx     : 46865224            Bytes Rx     : 2639672
  Pkts Tx      : 1635314             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              Hashing      : SHA1
  Encapsulation: Tunnel              PFS Group    : 5
  Rekey Int (T): 28800 Seconds       Rekey Left(T): 6282 Seconds
  Bytes Tx     : 1619268             Bytes Rx     : 872409912
  Pkts Tx      : 19277               Pkts Rx      : 1596809

hostname#
```

The following example shows the details of single session:

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

Index: 1 | Username: dbrownhi | Tunnel Group: bxbvpnlab | IP Addr: 192.168.2.70 | Public
IP: 10.86.5.114 | Protocol: IPSec | Encryption: AES128 | Login Time: 15:22:46 EDT Tue May
10 2005 |Duration: 6h:57m:40s | Bytes Tx: 0 | Bytes Rx: 598357 | Client Type: WinNT |
Client Ver: 4.6.00.0049 | Filter Name: | NAC Result: Accepted | Posture Token: Healthy ||

IKE Sessions: 1  | IPSec Sessions: 1  |  NAC Sessions: 1  |

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeysXauth | UDP Source Port: 500
| UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES |
Hashing: MD5 | Diffie-Hellman Group: 2 | Rekey Time Interval: 86400 Seconds| Rekey
Left(T): 61341 Seconds ||
```

```
Type: IPSec | Session ID: 2 | Local IP Addr: 0.0.0.0 | Remote IP Addr: 192.168.2.70 |
Encryption: AES128 | Hashing: SHA1 | Encapsulation: Tunnel | Rekey Time Interval: 28800
Seconds | Rekey Left(T): 26794 Seconds | Bytes Tx: 0 | Bytes Rx: 598357 | Packets Tx: 0 |
Packets Rx: 8044 | ||

Type: NAC | Revalidation Time Interval: 3000 Seconds | Time Until Next Revalidation: 286
Seconds | Status Query Time Interval: 600 Seconds | EAPoUDP Session Age: 2714 Seconds |
Hold-Off Time Remaining: 0 Seconds | Posture Token: Healthy | Redirect URL: www.cisco.com
||

AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : dbrownhi
Index        : 1
Assigned IP  : 192.168.2.70        Public IP    : 10.86.5.114
Protocol     : IPSec               Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                   Bytes Rx     : 604533
Client Type  : WinNT               Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy

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 1-6 explains these fields.

Table 1-6   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 security appliance.
Bytes Tx	Number of bytes transmitted to the remote peer or client by the security appliance.
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.

Table 1-6   show vpn-sessiondb Command Fields

Field	Description
Local IP Addr	IP address assigned to the local endpoint of the tunnel (that is the interface on the security appliance).
Login Time	Date and time (MMM DD HH:MM:SS) that the session logged in. Time is displayed in 24-hour notation.
NAC Result	State of Network Admission Control Posture Validation. It can be one of the following: • Accepted—The ACS successfully validated the posture of the remote host. • Rejected—The ACS could not successfully validate the posture of the remote host. • Exempted—The remote host is exempt from posture validation according to the Posture Validation Exception list configured on the security appliance. • Non-Responsive—The remote host did not respond to the EAPoUDP Hello message. • Hold-off—The 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 security appliance.
Packets Tx	Number of packets transmitted to the remote peer by the 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 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	Following posture validation or clientless authentication, the ACS downloads the access policy for the session to the security appliance. The Redirect URL is an optional part of the access policy payload. The 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 security appliance does not redirect HTTP and HTTPS requests from the remote host. Redirect URLs remain in force until either the IPSec session ends or until posture revalidation, for which the ACS downloads a new access policy that can contain a different redirect URL or no redirect URL.
Rekey Int (T)	Lifetime of the IPSec (IKE) SA encryption keys.
Rekey Left (T)	Lifetime remaining of the IPSec (IKE) SA encryption keys.

Table 1-6   *show vpn-sessiondb Command Fields*

Field	Description
Rekey Time Interval	Lifetime of the IPSec (IKE) SA encryption keys.
Remote IP Addr	IP address assigned to the remote endpoint of the tunnel (that is the interface on the remote peer).
Reval Int (T)	Revalidation Time Interval. Interval in seconds required between each successful posture validation.
Reval Left (T)	Time Until Next Revalidation. 0 if the last posture validation attempt was unsuccessful. Otherwise, the difference between the Revalidation Time Interval and the number of seconds since the last successful posture validation.
Revalidation Time Interval	Interval in seconds required between each successful posture validation.
Session ID	Identifier for the session component (subsession). Each SA has its own identifier.
Session Type	Type of session: LAN-to-LAN or Remote
SQ Int (T)	Status Query Time Interval. Time in seconds allowed between each successful posture validation or status query response and the next status query response. A status query is a request made by the 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 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 security appliance for UDP.
Username	User login name with which the session is established.

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 *groupname*	Filters the output to include session ratios only for the tunnel group you specify.
	protocol	Identifies the protocols you want to display. Protocols include:
		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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 IPSec, WebVPN, and Network Admission Control 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:

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

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

```
hostname# show vpn-sessiondb summary

Active Sessions:                        Session Information:
  IPSec LAN-to-LAN      : 0               Peak Concurrent       : 0
  IPSec Remote Access   : 0               IPSec Limit           : 750
  WebVPN                : 0               WebVPN Limit          : 500
  SSL VPN Client (SVC)  : 0               Cumulative Sessions   : 0
  Email Proxy           : 0
  Total Active Sessions : 0               Percent Session Load  : 0%
                                          VPN LB Mgmt Sessions  : 0

Active NAC Sessions:                    Cumulative NAC Sessions:
  Accepted              : 0               Accepted              : 0
  Rejected              : 0               Rejected              : 0
  Exempted              : 0               Exempted              : 0
  Non-responsive        : 0               Non-responsive        : 0
  Hold-off              : 0               Hold-off              : 0
  N/A                   : 0               N/A                   : 0
F1-asa1#
```

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.

Table 1-7 explains the fields in the Active Sessions and Session Information tables.

Table 1-7   *show vpn-sessiondb summary Command: Active Sessions and Session Information*
                    Fields

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

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:
	
	• Maximum number of IPSec and WebVPN sessions licensed.
	
	• Maximum number of sessions configured using the following commands:
	  – **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 1-6 explains the fields in the Active NAC Sessions and Total Cumulative NAC Sessions tables.

Table 1-8   *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 security appliance.
Hold-off	Number of peers for which the 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.

Table 1-8   show vpn-sessiondb summary Command: Active NAC Sessions and Total Cumulative NAC Sessions Fields

Field	Description
Non-responsive	Number of peers not responsive to Extensible Authentication Protocol (EAP) over UDP requests for posture validation. Peers on which no CTA is running do not respond to these requests. If the security appliance configuration supports clientless hosts, the Access Control Server downloads the access policy associated with clientless hosts to the security appliance for these peers. Otherwise, the 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.

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.
service-number	(Optional) Identification number of the web-cache service group being controlled by the cache. The number can be from 0 to 256. For web caches using Cisco Cache Engines, the reverse proxy service is indicated by a value of 99.
detail	(Optional) Displays information about the router and all web caches.
view	(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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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
asa1(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		
				Multiple	
	Routed	Transparent	Single	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

tunnel-group	(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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn group-url

To display the URLs for a specific tunnel-group or for all tunnel groups, use the **group-url** command in privileged EXEC mode.

show webvpn group-url [*tunnel-group*]

Syntax Description

tunnel-group	(Optional) Specifies a particular tunnel group for which to show the URLs.

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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

show webvpn sso-server

To display the operating statistics for a single sign-on server, use the **show webvpn sso-server** command in privileged EXEC mode. This is an SSO with CA SiteMinder command.

> **show webvpn sso-server** *name*

Syntax Description

name	Specifies the name of the SSO server. Minimum of 4 characters and maximum of 32 characters.

Defaults

No default values or behavior.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
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 reentering a username and password more than once. The **show webvpn sso-server** command displays operating statistics for any or all SSO servers configured.

If no SSO server name argument is entered, statistics on all SSO servers display.

Examples

The following example, entered in privileged EXEC mode, displays statistics for an 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(config-webvpn-sso-siteminder)#
```

Related Commands	Command	Description
	max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
	policy-server-secret	Creates a secret key used to encrypt authentication requests to an 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 security appliance makes SSO authentication requests.

show webvpn svc

To view the SVC installation, or to test a file to see if it is a valid SVC file, 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 for validity as an SVC 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**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 the existing SVC images that are configured for use.

Use the **image** *filename* option to test a file to see if it is a valid SVC image. If the file is not a valid SVC 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 SVC 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 15
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
SVC 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	Enables or requires the SVC for a specific group or user.
	svc enable	Enables the security appliance to download SVC files to remote computers.
	svc image	Causes the security appliance to load SVC files from flash memory to RAM, and specifies the order in which the security appliance downloads SVC files to the remote computer.

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:

State options:

- **static**—specifies **static** translations.
- **portmap**—specifies PAT global translations.
- **norandomseq**—specifies a **nat** or **static** translation with the **norondomseq** 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:

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	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 9.

Table 9   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 **vpnclient** configuration is enabled and the inside host is sending out DNS requests, the **show xlate** command may list multiple xlates for a static translation.

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.

Cisco Security Appliance Command Reference 7.2(2)