

show t

- show tcpstat, on page 2
- show tech-support, on page 5
- show telemetry, on page 9
- show terminal, on page 11
- show threat-detection memory, on page 13
- show threat-detection rate, on page 15
- show threat-detection scanning-threat, on page 18
- show threat-detection service, on page 20
- show threat-detection shun, on page 23
- show threat-detection statistics host, on page 25
- show threat-detection statistics port, on page 29
- show threat-detection statistics protocol, on page 32
- show threat-detection statistics top, on page 36
- show time-range, on page 45
- show tls-proxy, on page 46
- show track, on page 49
- show traffic, on page 50

show tcpstat

To display the status of the ASA TCP stack and the TCP connections that are terminated on the ASA (for debugging), use the **show tcpstat** command in privileged EXEC mode. This command supports IPv4 and IPv6 addresses.

show tcpstat

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the ASA. The TCP statistics displayed are described in Table 28 .

Table 1: TCP Statistics in the show tcpstat Command

Statistic	Description
tcb_cnt	Number of TCP users.
proxy_cnt	Number of TCP proxies. TCP proxies are used by user authorization.
tcp_xmt pkts	Number of packets that were transmitted by the TCP stack.
tcp_rcv good pkts	Number of good packets that were received by the TCP stack.
tcp_rcv drop pkts	Number of received packets that the TCP stack dropped.
tcp bad chksum	Number of received packets that had a bad checksum.
tcp user hash add	Number of TCP users that were added to the hash table.
tcp user hash add dup	Number of times a TCP user was already in the hash table when trying to add a new user.

Statistic	Description
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.
tcp user srch hash miss	Number of times a TCP user was not found in the hash table when searching.
tcp user hash delete	Number of times that a TCP user was deleted from the hash table.
tcp user hash delete miss	Number of times that a TCP user was not found in the hash table when trying to delete the user.
lip	Local IP address of the TCP user.
fip	Foreign IP address of the TCP user.
lp	Local port of the TCP user.
fp	Foreign port of the TCP user.
st	State (see RFC 793) of the TCP user. The possible values are as follows: 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	Length of the retransmit queue of the TCP user.
inqlen	Length of the input queue of the TCP user.
tw_timer	Value of the time_wait timer (in milliseconds) of the TCP user.
to_timer	Value of the inactivity timeout timer (in milliseconds) of the TCP user.
cl_timer	Value of the close request timer (in milliseconds) of the TCP user.
per_timer	Value of the persist timer (in milliseconds) of the TCP user.
rt_timer	Value of the retransmit timer (in milliseconds) of the TCP user.
tries	Retransmit count of the TCP user.

Examples

This example shows how to display the status of the TCP stack on the ASA:

```
ciscoasa# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160
tcp_xmt pkts = 540591
```

```
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0
lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

Related Commands

Command	Description
show conn	Displays the connections used and those that are available.

show tech-support

To display the information that is used for diagnosis by technical support analysts, use the **show tech-support** command in privileged EXEC mode.

show tech-support [**detail** [**vsn**] | **file** | **no-config** | **no-config** | **performance**]

Syntax Description

detail	(Optional) Lists detailed information.
file	(Optional) Writes the output of the command to a file. File system types include the following: disk0:, disk1:, ftp:, scp:, smb:, and tftp:.
no-config	(Optional) Excludes the output of the running configuration.
performance	(Optional) Displays performance information.
vsn	(Optional) Includes additional ASA1000V Policy Agent technical support information, which is redirected to a file.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The **detail** and **file** keywords were added.
7.2(1)	The output was enhanced to display more detailed information about processes that hog the CPU.
9.1(2)	The output was enhanced to include information from the **show environment** command.
9.1(3)	The output was enhanced to include information from the **show memory detail,** **show memory top-usage,** and **show vlan** commands.
9.2(1)	The output was enhanced to include information from the **show memory detail** , **show cpu detail** , **show blocks queue history core-local** , **show asp drop** , and **show asp event dp-cp** , **show cpu usage history** , and **show traffic summary** commands. The output from the **show kernel cgroup-controller detail** command was removed.The **performance** and **vsn** keywords were added.
9.2(1)	The output was enhanced to include information from the **show vlan** command.

Release	Modification
9.1(7)/9.3(1)	The **show tech-support** command now includes **show resource usage count all 1** output, including information about xlates, conns, inspects, syslogs, and so on. This information is helpful for diagnosing performance issues.
9.3(2)	The **show route-summary** command output was added to the **show tech-support detail** command.
9.4(1)	The **show tech-support** command output includes the most recent 50 lines of generated syslogs. Note that you must enable the **logging buffer** command to enable these results to appear.
9.1(7)/9.4(3)/9.5(2)	The **show tech-support** command now: • Includes **dir all-filesystems** output—This output can be helpful in the following cases: • SSL VPN configuration: check if the required resources are on the ASA • Crash: check for the date timestamp and presence of a crash file • Removes the **show kernel cgroup-controller detail** output—This command output will remain in the output of **show tech-support detail** .
9.7.(1)	The **show tech-support** command was updated for the following changes: • The output was enhanced to include crashinfo statistics like **thread name** , **registry content** , **timestamp** , and **traceback** from the crashed thread. The output from **Saved crash** timestamp was removed. • The output was enhanced to include **show ipsec stats** , **show crypto ikev1 stats** , and **show crypto ikev2 stats** commands. These commands are used to gather VPN statistics for troubleshooting purposes. • The **show tech-support** command now includes **show vm** output. It determines the hypervisor on which the ASA Virtual is currently running. This information is helpful for performing multiple automated checks on virtual platforms. • The **show tech-support** command now includes **show module detail** command. This command provides information about multiple modules, which is helpful for troubleshooting various connectivity and status issues.
9.12(1)	The output of **show ipv6 interface, show aaa-server, and show fragment** was added to the output of **show tech-support** .
9.13(1)	The **show flow-offload info detail, show flow-offload statistics** , and **show asp table socket** commands were added.
9.14(1)	The **show ssl objects and show ssl errors was added to the output of show tech-support.** Also in 9.12(4)

Release	Modification
9.16(1)	The **show tech-support** command is enhanced for the following changes: • **showcontroller** command output that includes DPDK log messages from the last boot. • **meminfo** statistics about the virtual machine's (VM) free and used memory, shared memory, and buffers. • **cmdline** statistics about the options and arguments passed during boot.
9.17(1)	The output from **show access-list element-count** and **show asp rule-engine** were added. The output of the **show tech-support** command now includes the current DPDK memory pool statistics.
9.20(2)	The output of this command includes the output for **statistics all**,**statistics events**,**statistics np-clients**,**statistics cp-clients**, and **statistics bulk-sync** statistics.

Usage Guidelines

The show tech-support command lets you list information that technical support analysts need to help you diagnose problems. This command combines the output from the show commands that provide the most information to a technical support analyst.

Examples

The following example shows how to save the **show tech-support** output to a file on disk0. The output is extremely long, so if you send the results to your screen, it will take a long time to page through the results.

```
ciscoasa# show tech-support file disk0:tech-support-output.txt

ciscocasa#
```

Note Do not use the **terminal pager 0** command while running any show commands, as it can lead to a huge CPU load. The CPU overload can result in ASA communication failure. Hence, use the default config terminal pager settings (25 lines).

Related Commands

Command	Description
show clock	Displays the clock for use with the Syslog Server (PFSS) and the Public Key Infrastructure (PKI) protocol.
show conn count	Displays the connections used and available.
show cpu	Display the CPU utilization information.
show failover	Displays the status of a connection and which ASA is active
show memory	Displays a summary of the maximum physical memory and current free memory that is available to the operating system.

Command	Description
show perfmon	Displays information about the performance of the ASA
show processes	Displays a list of the processes that are running.
show running-config	Displays the configuration that is currently running on the ASA.
show xlate	Displays information about the translation slot.

show telemetry

To view the telemetry data, use the **show telemetry** command in privileged EXEC mode with one of the keywords. It displays the data in JSON format.

show telemetry [**history | last-report | sample**]

Syntax Description

history	(Optional) Shows the past 100 events related to telemetry configuration and activities.
last-report	(Optional) Shows the latest telemetry data sent to FXOS in JSON format.
sample	(Optional) Shows the instantly generated telemetry data in JSON format.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.13(1)	Command was introduced.

Usage Guidelines

The service telemetry command is enabled by default. You can choose to view the last sent telemetry data or the last 100 events related to telemetry configuration and activities.

Examples

The following is sample output from the **show telemetry history** command:

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 1. Telemetry support on the chassis: disabled
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE connector
 status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
```

Related Commands

Command	Description
no service telemetry	Disables the telemetry service.
show running-config	Displays only the non-default telemetry settings that is configured.

Command	Description
show running-config all	Displays the configured telemetry settings.

show terminal

To show the terminal settings for the current CLI session, use the **show terminal** command in privileged EXEC mode.

show terminal

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	Command added.

Usage Guidelines

Set the terminal properties with the following commands:

- **terminal interactive**—Enables help in the current CLI session when you enter **?** at the CLI.
- **terminal monitor**—Allows syslog messages to show in the current CLI session.
- **terminal width**—Sets the width for displaying information during console sessions.

The **show terminal** command does not show the **terminal pager** setting.

Examples

The following is sample output from the **show terminal** command:

```
ciscoasa# show terminal
Width = 80, no monitor
terminal interactive
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
pager	Sets the number of lines to display in a Telnet session before the “---more---” prompt. This command is saved to the configuration.

Command	Description
show running-config terminal	Displays the current terminal settings.
terminal interactive	Enables help in the current CLI session when you enter **?** at the CLI.
terminal monitor	Allows syslog messages to show in the current CLI session.
terminal pager	Sets the number of lines to display in a Telnet session before the "---more---" prompt. This command is not saved to the configuration.
terminal width	Sets the width for displaying information during console sessions.

show threat-detection memory

To show the memory used by advanced threat detection statistics, which are enabled by the **threat-detection statistics** command, use the **show threat-detection memory** command in privileged EXEC mode.

show threat-detection memory

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.3(1)	This command was added.

Usage Guidelines

Some statistics can use a lot of memory and can affect ASA performance. This command lets you monitor memory usage so you can adjust your configuration if necessary.

Examples

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

```
ciscoasa# show threat-detection memory
Cached chunks:
       CACHE TYPE             BYTES USED
TD Host                         70245888
TD Port                             2724
TD Protocol                         1476
TD ACE                               728
TD Shared counters                 14256
============================
Subtotal TD Chunks              70265072
Regular memory                 BYTES USED
TD Port                             33824
TD Control block                   162064
============================
Subtotal Regular Memory            195888
Total TD memory:                70460960
```

Related Commands

Command	Description
show threat-detection statistics host	Shows the host statistics.

Command	Description
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection statistics	Enables advanced threat-detection statistics.

show threat-detection rate

When you enable basic threat detection using the **threat-detection basic-threat** command, you can view statistics using the **show threat-detection rate** command in privileged EXEC mode.

show threat-detection rate [**min-display-rate** *min_display_rate*] [**acl-drop | bad-packet-drop | conn-limit-drop | dos-drop | fw-drop | icmp-drop | inspect-drop | interface-drop | scanning-threat | syn-attack**]

Syntax Description

acl-drop	(Optional) Shows the rate for dropped packets caused by denial by access lists.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
bad-packet-drop	(Optional) Shows the rate for dropped packets caused by denial by a bad packet format (such as invalid-ip-header or invalid-tcp-hdr-length).
conn-limit-drop	(Optional) Shows the rate for dropped packets caused by the connection limits being exceeded (both system-wide resource limits, and limits set in the configuration).
dos-drop	(Optional) Shows the rate for dropped packets caused by a detected DoS attack (such as an invalid SPI, Stateful Firewall check failure).
fw-drop	(Optional) Shows the rate for dropped packets caused by basic firewall check failure. This option is a combined rate that includes all firewall-related packet drops in this command. It does not include non-firewall-related drops such as **interface-drop**, **inspect-drop**, and **scanning-threat**.
icmp-drop	(Optional) Shows the rate for dropped packets caused by denial by suspicious ICMP packets detected.
inspect-drop	(Optional) Shows the rate limit for dropped packets caused by packets failing application inspection.
interface-drop	(Optional) Shows the rate limit for dropped packets caused by an interface overload.
scanning-threat	(Optional) Shows the rate for dropped packets caused by a scanning attack detected. This option monitors scanning attacks; for example, the first TCP packet is not a SYN packet, or the TCP connection failed the 3-way handshake. Full scanning threat detection (see the **threat-detection scanning-threat** command) takes this scanning attack rate information and acts on it by classifying hosts as attackers and automatically shunning them, for example.
syn-attack	(Optional) Shows the rate for dropped packets caused by an incomplete session, such as TCP SYN attack or UDP session with no return data attack.

Command Default

If you do not specify an event type, all events are shown.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 10 minutes, then the burst interval is 10 seconds. If the last burst interval was from 3:00:00 to 3:00:10, and you use the **show** command at 3:00:15, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 59 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

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

```
ciscoasa# show threat-detection rate
                        Average(eps)    Current(eps) Trigger         Total events
  10-min ACL  drop:                0               0       0                   16
  1-hour ACL  drop:                0               0       0                  112
  1-hour SYN attck:                5               0       2                21438
  10-min  Scanning:                0               0      29                  193
  1-hour  Scanning:              106               0      10               384776
  1-hour Bad  pkts:               76               0       2               274690
  10-min  Firewall:                0               0       3                   22
  1-hour  Firewall:               76               0       2               274844
  10-min DoS attck:                0               0       0                    6
  1-hour DoS attck:                0               0       0                   42
```

```
10-min Interface:                0              0       0                204
1-hour Interface:               88              0       0             318225
```

Related Commands

Command	Description
clear threat-detection rate	Clears basic threat detection statistics.
show running-config all threat-detection	Shows the threat detection configuration, including the default rate settings if you did not configure them individually.
threat-detection basic-threat	Enables basic threat detection.
threat-detection rate	Sets the threat detection rate limits per event type.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection scanning-threat

If you enable scanning threat detection with the **threat-detection scanning-threat** command, then view the hosts that are categorized as attackers and targets using the **show threat-detection scanning-threat** command in privileged EXEC mode.

show threat-detection scanning-threat [**attacker** | **target**]

Syntax Description

attacker	(Optional) Shows attacking host IP addresses.
target	(Optional) Shows targeted host IP addresses.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	The display was modified to include "& Subnet List" in the heading text.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.
9.0	Interface information was added to the output.

Examples

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

```
ciscoasa# show threat-detection scanning-threat
Latest Target Host & Subnet List:
    192.168.1.0 (l2l)
    192.168.1.249 (l2l)
Latest Attacker Host & Subnet List:
    192.168.10.234 (outside)
    192.168.10.0 (outside)
    192.168.10.2 (outside)
    192.168.10.3 (outside)
    192.168.10.4 (outside)
    192.168.10.5 (outside)
    192.168.10.6 (outside)
    192.168.10.7 (outside)
```

```
192.168.10.8 (outside)
192.168.10.9 (outside)
```

Related Commands

Command	Description
clear threat-detection shun	Releases hosts from being shunned.
show threat-detection shun	Shows the currently shunned hosts.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection service

To view the status and statistics for Threat Detection for VPN Services, use the **show threat-detection service** command in privileged EXEC mode.

show threat-detection service [*service*] [**details** | **entries**]

Syntax Description

details	(Optional.) Show both service details and service entries.
entries	(Optional.) Shows only the entries being tracked. For example, the IP addresses that have had failed authentication attempts.
service	(Optional.) Show information for the specified service only. Enter one of the following: • **remote-access-authentication** • **remote-access-client-initiations** • **invalid-vpn-access**

Command Default

Details for all services are displayed.

Command Modes

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

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

Command History

Release	Modification
9.16(4), 9.20(3)	This command was introduced.

Usage Guidelines

Based on selected options, the display output shows the following:

- The name of the service
- The state of the service: enabled or disabled
- The service hold-down setting
- The service threshold setting
- Service action statistics
  - Failed—A failure occurrence when processing the reported occurrence.

- Blocking—The reported occurrence is within the hold-down period and the threshold was met or exceeded. As a result, the service automatically installed a shun to block the mischievous peer.
- Recording—The reported occurrence is outside of the hold-down period, or the threshold was met or exceeded. As a result, the service will record the occurrence.
- Unsupported—The reported occurrence does not currently support automatic shunning.
- Disabled—An occurrence was reported; but the service has been disabled.

Example

The following example shows that all services are enabled, and potential attackers are being tracked for the remote-access-authentication service.

```
ciscoasa# show threat-detection service
Service: invalid-vpn-access
    State     : Enabled
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 3
Name: remote-access-client-initiations
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

The following is an example of the **show threat-detection service entries** command.

```
ciscoasa# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
```

```
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

The following is an example of the **show threat-detection service details** command.

```
ciscoasa# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1        721           0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

Related Commands

Command	Description
clear shun	Removes all shuns.
clear threat-detection service	Clears threat detection service entries and statistics.
[no]shun	Shuns an address, or clears the shun on a specific address.
threat-detection service	Configures Threat Detection for VPN Services.

show threat-detection shun

If you enable scanning threat detection with the **threat-detection scanning-threat** command, and you automatically shun attacking hosts, then view the currently shunned hosts using the **show threat-detection shun** command in privileged EXEC mode.

show threat-detection shun

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.
9.0	Interface information was added to the output.

Usage Guidelines

To release a host from being shunned, use the **clear threat-detection shun** command.

Examples

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

```
ciscoasa# show threat-detection shun
Shunned Host List:
(outside) src-ip=10.0.0.13 255.255.255.255
(inside) src-ip=10.0.0.13 255.255.255.255
```

Related Commands

Command	Description
clear threat-detection shun	Releases hosts from being shunned.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
show threat-detection statistics top	Shows the top 10 statistics.

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.

show threat-detection statistics host

After you enable threat statistics with the **threat-detection statistics host** command, view host statistics using the **show threat-detection statistics host** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **host** [*ip_address* [*mask*]]

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval

presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

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

```
ciscoasa# show threat-detection statistics host
                        Average(eps)    Current(eps) Trigger         Total events
Host:10.0.0.1: tot-ses:289235 act-ses:22571 fw-drop:0 insp-drop:0 null-ses:21438 bad-acc:0
  1-hour Sent byte:               2938               0       0             10580308
  8-hour Sent byte:                367               0       0             10580308
 24-hour Sent byte:                122               0       0             10580308
  1-hour Sent pkts:                 28               0       0               104043
  8-hour Sent pkts:                  3               0       0               104043
 24-hour Sent pkts:                  1               0       0               104043
  20-min Sent drop:                  9               0       1                10851
  1-hour Sent drop:                  3               0       1                10851
  1-hour Recv byte:               2697               0       0              9712670
  8-hour Recv byte:                337               0       0              9712670
 24-hour Recv byte:                112               0       0              9712670
  1-hour Recv pkts:                 29               0       0               104846
  8-hour Recv pkts:                  3               0       0               104846
 24-hour Recv pkts:                  1               0       0               104846
  20-min Recv drop:                 42               0       3                50567
  1-hour Recv drop:                 14               0       1                50567
Host:10.0.0.0: tot-ses:1 act-ses:0 fw-drop:0 insp-drop:0 null-ses:0 bad-acc:0
  1-hour Sent byte:                  0               0       0                  614
  8-hour Sent byte:                  0               0       0                  614
 24-hour Sent byte:                  0               0       0                  614
  1-hour Sent pkts:                  0               0       0                    6
  8-hour Sent pkts:                  0               0       0                    6
 24-hour Sent pkts:                  0               0       0                    6
  20-min Sent drop:                  0               0       0                    4
  1-hour Sent drop:                  0               0       0                    4
  1-hour Recv byte:                  0               0       0                  706
  8-hour Recv byte:                  0               0       0                  706
 24-hour Recv byte:                  0               0       0                  706
  1-hour Recv pkts:                  0               0       0                    7
```

Table 13-2 shows each field description.

Table 2: show threat-detection statistics host Fields

Field	Description
Host	Shows the host IP address.
tot-ses	Shows the total number of sessions for this host since it was added to the database.
act-ses	Shows the total number of active sessions that the host is currently involved in.

Field	Description
fw-drop	Shows the number of firewall drops. Firewall drops is a combined rate that includes all firewall-related packet drops tracked in basic threat detection, including access list denials, bad packets, exceeded connection limits, DoS attack packets, suspicious ICMP packets, TCP SYN attack packets, and UDP session with no return data attack packets. It does not include non-firewall-related drops such as interface overload, packets failed at application inspection, and scanning attack detected.
insp-drop	Shows the number of packets dropped because they failed application inspection.
null-ses	Shows the number of null sessions, which are TCP SYN sessions that did not complete within the 30-second timeout, and UDP sessions that did not have any data sent by its server 3 seconds after the session starts.
bad-acc	Shows the number of bad access attempts to host ports that are in a closed state. When a port is determined to be in a null session (see above), the port state of the host is set to HOST_PORT_CLOSE. Any client accessing the port of the host is immediately classified as a bad access without the need to wait for a timeout.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Field	Description
20-min, 1-hour, 8-hour, and 24-hour	By default, there are three rate intervals shown. You can reduce the number of rate intervals using the **threat-detection statistics host number-of-rate** command. Because host statistics use a lot of memory, reducing the number of rate intervals from the default of 3 reduces the memory usage. If you set this keyword to 1, then only the shortest rate interval statistics are maintained. If you set the value to 2, then the two shortest intervals are maintained.
Sent byte	Shows the number of successful bytes sent from the host.
Sent pkts	Shows the number of successful packets sent from the host.
Sent drop	Shows the number of packets sent from the host that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the host.
Recv pkts	Shows the number of successful packets received by the host.
Recv drop	Shows the number of packets received by the host that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics port

After you enable threat statistics with the **threat-detection statistics port** command, view TCP and UDP port statistics using the **show threat-detection statistics port** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min-display-rate*] **port** [*start_port* [*-end_port*]]

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes,

then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

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

```
ciscoasa# show threat-detection statistics port
                          Average(eps)    Current(eps) Trigger         Total events
80/HTTP: tot-ses:310971 act-ses:22571
  1-hour Sent byte:               2939              0       0             10580922
  8-hour Sent byte:                367          22043       0             10580922
 24-hour Sent byte:                122           7347       0             10580922
  1-hour Sent pkts:                 28              0       0               104049
  8-hour Sent pkts:                  3            216       0               104049
 24-hour Sent pkts:                  1             72       0               104049
  20-min Sent drop:                  9              0       2                10855
  1-hour Sent drop:                  3              0       2                10855
  1-hour Recv byte:               2698              0       0              9713376
  8-hour Recv byte:                337          20236       0              9713376
 24-hour Recv byte:                112           6745       0              9713376
  1-hour Recv pkts:                 29              0       0               104853
  8-hour Recv pkts:                  3            218       0               104853
 24-hour Recv pkts:                  1             72       0               104853
  20-min Recv drop:                 24              0       2                29134
  1-hour Recv drop:                  8              0       2                29134
```

Table 13-2 shows each field description.

Table 3: show threat-detection statistics port Fields

Field	Description
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00

Field	Description
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
port_number /*port_name*	Shows the port number and name where the packet or byte was sent, received, or dropped.
tot-ses	Shows the total number of sessions for this port.
act-ses	Shows the total number of active sessions that the port is currently involved in.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the port.
Sent pkts	Shows the number of successful packets sent from the port.
Sent drop	Shows the number of packets sent from the port that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the port.
Recv pkts	Shows the number of successful packets received by the port.
Recv drop	Shows the number of packets received by the port that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics host	Shows the host statistics.
show threat-detection statistics protocol	Shows the protocol statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics protocol

After you enable threat statistics with the **threat-detection statistics protocol** command, view IP protocol statistics using the **show threat-detection statistics protocol** command in privileged EXEC mode. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **protocol** [*protocol_number* | *protocol_name*]

Syntax Description

protocol_number	(Optional) Shows statistics for a specific protocol number, between 0 and 255.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
protocol_name	(Optional) Shows statistics for a specific protocol name: • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

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

```
ciscoasa# show threat-detection statistics protocol
                        Average(eps)    Current(eps) Trigger         Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                0               0       0                 1000
  8-hour Sent byte:                0               2       0                 1000
 24-hour Sent byte:                0               0       0                 1000
  1-hour Sent pkts:                0               0       0                   10
  8-hour Sent pkts:                0               0       0                   10
 24-hour Sent pkts:                0               0       0                   10
```

Table 13-2 shows each field description.

Table 4: show threat-detection statistics protocol Fields

Field	Description
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
protocol_number /*protocol_name*	Shows the protocol number and name where the packet or byte was sent, received, or dropped.
tot-ses	Not currently used.
act-ses	Not currently used.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the protocol.
Sent pkts	Shows the number of successful packets sent from the protocol.
Sent drop	Shows the number of packets sent from the protocol that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the protocol.

Field	Description
Recv pkts	Shows the number of successful packets received by the protocol.
Recv drop	Shows the number of packets received by the protocol that were dropped because they were part of a scanning attack.

Related Commands

Command	Description
threat-detection scanning-threat	Enables scanning threat detection.
show threat-detection statistics top	Shows the top 10 statistics.
show threat-detection statistics port	Shows the port statistics.
show threat-detection statistics host	Shows the host statistics.
threat-detection statistics	Enables threat statistics.

show threat-detection statistics top

After you enable threat statistics with the **threat-detection statistics** command, view the top 10 statistics using the **show threat-detection statistics top** command in privileged EXEC mode. If you did not enable the threat detection statistics for a particular type, then you cannot view those statistics with this command. Threat detection statistics show both allowed and dropped traffic rates.

show threat-detection statistics [**min-display-rate** *min_display_rate*] **top** [[**access-list | host | port-protocol**] [**rate-1 | rate-2 | rate-3**] **| tcp-intercept** [**all**] [**detail**] [**long**]]

Syntax Description

access-list	(Optional) Shows the top 10 ACEs that that match packets, including both permit and deny ACEs. Permitted and denied traffic are not differentiated in this display. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command.
all	(Optional) For TCP Intercept, shows the history data of all the traced servers.
detail	(Optional) For TCP Intercept, shows history sampling data.
host	(Optional) Shows the top 10 host statistics for each fixed time period. **Note** Due to the threat detection algorithm, an interface used for a failover link or state link could appear as one of the top 10 hosts. This occurrence is more likely when you use one interface for both the failover and state link. This is expected behavior, and you can ignore this IP address in the display.
long	(Optional) Shows the statistical history in a long format, with the real IP address and the untranslated IP address of the server.
min-display-rate *min_display_rate*	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the *min_display_rate* between 0 and 2147483647.
port-protocol	(Optional) Shows the top 10 combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols; TCP and UDP ports are, however, included in the display for ports. If you only enable statistics for one of these types, port or protocol, then you will only view the enabled statistics.
rate-1	(Optional) Shows the statistics for the smallest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-1** keyword, the ASA shows only the 1 hour time interval.
rate-2	(Optional) Shows the statistics for the middle fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-2** keyword, the ASA shows only the 8 hour time interval.

rate-3	(Optional) Shows the statistics for the largest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the **rate-3** keyword, the ASA shows only the 24 hour time interval.
tcp-intercept	Shows TCP Intercept statistics. The display includes the top 10 protected servers under attack.

Command Default

If you do not specify an event type, all events are shown.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.0(4)	The **tcp-intercept** keyword was added.
8.2(1)	The burst rate interval changed from 1/60th to 1/30th of the average rate.
8.2(2)	The **long** keyword was added for **tcp-intercept** . For threat events, the severity level was changed from a warning to a notification. Threat events can be triggered every five minutes.

Usage Guidelines

The display output shows the following:

- The average rate in events/sec over fixed time periods.
- The current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger
- The number of times the rates were exceeded (for dropped traffic statistics only)
- The total number of events over the fixed time periods.

The ASA computes the event counts 30 times over the average rate interval; in other words, the ASA checks the rate at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output.

The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Examples

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

```
ciscoasa# show threat-detection statistics top access-list
                    Top     Average(eps)     Current(eps) Trigger         Total events
  1-hour ACL hits:
               100/3[0]              173                0       0                623488
               200/2[1]               43                0       0                156786
               100/1[2]               43                0       0                156786
  8-hour ACL hits:
               100/3[0]               21             1298       0                623488
               200/2[1]                5              326       0                156786
               100/1[2]                5              326       0                156786
```

Table 13-2 shows each field description.

Table 5: show threat-detection statistics top access-list Fields

Field	Description
Top	Shows the ranking of the ACE within the time period, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 ACEs might be listed.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the **show** command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.
Current(eps)	Shows the current burst rate in events/sec over the last completed burst interval, which is 1/30th of the average rate interval or 10 seconds, whichever is larger. For the example specified in the Average(eps) description, the current rate is the rate from 3:19:30 to 3:20:00.
Trigger	This column is always 0, because there are no rate limits triggered by access list traffic; denied and permitted traffic are not differentiated in this display. If you enable basic threat detection using the **threat-detection basic-threat** command, you can track access list denies using the **show threat-detection rate access-list** command.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the ASA calculates the total events as the last 29 complete intervals, plus the events so far in the unfinished burst interval. This exception lets you monitor a large increase in events in real time.

Field	Description
1-hour, 8-hour	Shows statistics for these fixed rate intervals.
acl_name /*line_number*	Shows the access list name and line number of the ACE that caused the denies.

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

```
ciscoasa# show threat-detection statistics top access-list rate-1
                    Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour ACL hits:
              100/3[0]             173               0       0               623488
              200/2[1]              43               0       0               156786
              100/1[2]              43               0       0               156786
```

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

```
ciscoasa# show threat-detection statistics top port-protocol
Top          Name   Id    Average(eps)    Current(eps) Trigger      Total events
  1-hour Recv byte:
 1         gopher   70              71               0       0          32345678
 2  btp-clnt/dhcp   68              68               0       0          27345678
 3         gopher   69              65               0       0          24345678
 4    Protocol-96 * 96              63               0       0          22345678
 5      Port-7314 7314              62               0       0          12845678
 6 BitTorrent/trc 6969              61               0       0          12645678
 7     Port-8191-65535              55               0       0          12345678
 8           SMTP  366              34               0       0           3345678
 9         IPinIP *  4              30               0       0           2345678
10          EIGRP * 88              23               0       0           1345678
  1-hour Recv pkts:
...
...
  8-hour Recv byte:
...
...
  8-hour Recv pkts:
...
...
 24-hour Recv byte:
...
...
 24-hour Recv pkts:
...
...
Note: Id preceded by * denotes the Id is an IP protocol type
```

Table 13-6 shows each field description.

Table 6: show threat-detection statistics top port-protocol Fields

Field	Description
Top	Shows the ranking of the port or protocol within the time period/type of statistic, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 ports/protocols might be listed.
Name	Shows the port/protocol name.
Id	Shows the port/protocol ID number. The asterisk (*) means the ID is an IP protocol number.
Average(eps)	See the description in Table 13-2.
Current(eps)	See the description in Table 13-2.
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	See the description in Table 13-2.
Time_interval Sent byte	Shows the number of successful bytes sent from the listed ports and protocols for each time period.
Time_interval Sent packet	Shows the number of successful packets sent from the listed ports and protocols for each time period.
Time_interval Sent drop	Shows the number of packets sent for each time period from the listed ports and protocols that were dropped because they were part of a scanning attack.
Time_interval Recv byte	Shows the number of successful bytes received by the listed ports and protocols for each time period.
Time_interval Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
Time_interval Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
port_number /*port_name*	Shows the port number and name where the packet or byte was sent, received, or dropped.
protocol_number /*protocol_name*	Shows the protocol number and name where the packet or byte was sent, received, or dropped.

Examples

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

```
ciscoasa# show threat-detection statistics top host
                    Top    Average(eps)    Current(eps) Trigger         Total events
  1-hour Sent byte:
          10.0.0.1[0]            2938               0       0             10580308
  1-hour Sent pkts:
          10.0.0.1[0]              28               0       0               104043
  20-min Sent drop:
          10.0.0.1[0]               9               0       1                10851
  1-hour Recv byte:
          10.0.0.1[0]            2697               0       0              9712670
  1-hour Recv pkts:
          10.0.0.1[0]              29               0       0               104846
  20-min Recv drop:
          10.0.0.1[0]              42               0       3                50567
  8-hour Sent byte:
          10.0.0.1[0]             367               0       0             10580308
  8-hour Sent pkts:
          10.0.0.1[0]               3               0       0               104043
  1-hour Sent drop:
          10.0.0.1[0]               3               0       1                10851
  8-hour Recv byte:
          10.0.0.1[0]             337               0       0              9712670
  8-hour Recv pkts:
          10.0.0.1[0]               3               0       0               104846
  1-hour Recv drop:
          10.0.0.1[0]              14               0       1                50567
 24-hour Sent byte:
          10.0.0.1[0]             122               0       0             10580308
 24-hour Sent pkts:
          10.0.0.1[0]               1               0       0               104043
 24-hour Recv byte:
          10.0.0.1[0]             112               0       0              9712670
 24-hour Recv pkts:
          10.0.0.1[0]               1               0       0               104846
```

Table 13-7 shows each field description.

Table 7: show threat-detection statistics top host Fields

Field	Description
Top	Shows the ranking of the host within the time period/type of statistic, from [0] (highest count) to [9] (lowest count). You might not have enough statistics for all 10 positions, so less then 10 hosts might be listed.
Average(eps)	See the description in Table 13-2.
Current(eps)	See the description in Table 13-2.
Trigger	See the description in Table 13-2.
Total events	See the description in Table 13-2.
Time_interval Sent byte	Shows the number of successful bytes sent to the listed hosts for each time period.
Time_interval Sent packet	Shows the number of successful packets sent to the listed hosts for each time period.

Field	Description
Time_interval Sent drop	Shows the number of packets sent for each time period to the listed hosts that were dropped because they were part of a scanning attack.
Time_interval Recv byte	Shows the number of successful bytes received by the listed hosts for each time period.
Time_interval Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
Time_interval Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
host_ip_address	Shows the host IP address where the packet or byte was sent, received, or dropped.

Examples

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

```
ciscoasa# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

Table 13-8 shows each field description.

Table 8: show threat-detection statistics top tcp-intercept Fields

Field	Description
Monitoring window size:	Shows the period of time over which the ASA samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command. The ASA samples data 30 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 30.
rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.

Field	Description
server_ip:port	Shows the server IP address and the port on which it is being attacked.
interface	Shows the interface through which the server is being attacked.
avg_rate	Shows the average rate of attack, in attacks per second over the sampling period
current_rate	Shows the current attack rate, in attacks per second.
total	Shows the total number of attacks.
attacker_ip	Shows the attacker IP address.
(*last_attack_time* ago)	Shows when the last attack occurred.

Examples

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

```
ciscoasa# show threat-detection statistics top tcp-intercept long
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port (Real IP:Real Port)> <Interface> <Ave Rate> <Cur Rate> <Total> <Source
 IP (Last Attack Time)>
------------------------------------------------------------------------------
1    10.1.0.2:6025 (209.165.200.227:6025) inside 18 709 33911 10.0.0.201 (0 secs ago)
2    10.1.0.2:6026 (209.165.200.227:6026) inside 18 709 33911 10.0.0.201 (0 secs ago)
3    10.1.0.2:6027 (209.165.200.227:6027) inside 18 709 33911 10.0.0.201 (0 secs ago)
4    10.1.0.2:6028 (209.165.200.227:6028) inside 18 709 33911 10.0.0.201 (0 secs ago)
5    10.1.0.2:6029 (209.165.200.227:6029) inside 18 709 33911 10.0.0.201 (0 secs ago)
6    10.1.0.2:6030 (209.165.200.227:6030) inside 18 709 33911 10.0.0.201 (0 secs ago)
7    10.1.0.2:6031 (209.165.200.227:6031) inside 18 709 33911 10.0.0.201 (0 secs ago)
8    10.1.0.2:6032 (209.165.200.227:6032) inside 18 709 33911 10.0.0.201 (0 secs ago)
9    10.1.0.2:6033 (209.165.200.227:6033) inside 18 709 33911 10.0.0.201 (0 secs ago)
10   10.1.0.2:6034 (209.165.200.227:6034) inside 18 709 33911 10.0.0.201 (0 secs ago)
```

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

```
ciscoasa# show threat-detection statistics top tcp-intercept detail
Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
     Sampling History (30 Samplings):
             95348      95337      95341      95339      95338      95342
             95337      95348      95342      95338      95339      95340
             95339      95337      95342      95348      95338      95342
             95337      95339      95340      95339      95347      95343
             95337      95338      95342      95338      95337      95342
             95348      95338      95342      95338      95337      95343
             95337      95349      95341      95338      95337      95342
             95338      95339      95338      95350      95339      95570
             96351      96351      96119      95337      95349      95341
             95338      95337      95342      95338      95338      95342
......
```

Table 13-9 shows each field description.

Table 9: show threat-detection statistics top tcp-intercept detail Fields

Field	Description
Monitoring window size:	Shows the period of time over which the ASA samples data for statistics. The default is 30 minutes. You can change this setting using the **threat-detection statistics tcp-intercept rate-interval** command. The ASA samples data 30 times during this interval.
Sampling interval:	Shows the interval between samples. This value is always the rate interval divided by 30.
rank	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
server_ip:port	Shows the server IP address and the port on which it is being attacked.
interface	Shows the interface through which the server is being attacked.
avg_rate	Shows the average rate of attack, in attacks per second over the rate interval set by the **threat-detection statistics tcp-intercept rate-interval** command (by default, the rate interval is 30 minutes). The ASA samples the data every 30 seconds over the rate interval.
current_rate	Shows the current attack rate, in attacks per second.
total	Shows the total number of attacks.
attacker_ip or <various> Last: *attacker_ip*	Shows the attacker IP address. If there is more than one attacker, then "<various>" displays followed by the last attacker IP address.
(*last_attack_time* ago)	Shows when the last attack occurred.
sampling data	Shows all 30 sampling data values, which show the number of attacks at each inerval.

Related Commands

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

show time-range

To display the configuration of all time range objects, use the **show time-range** command in privileged EXEC mode.

show time-range [[*name*]]

Syntax Description

name (Optional) Shows information for this time range object only.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Examples

This example shows how to display the configuration of the time range objects. In this example, there is one object, which is named work-hours. Inactive means that the object is not being used.

```
ciscoasa# show time-range

time-range entry: work-hours (inactive)
   periodic weekdays 9:00 to 17:00
```

Related Commands

Command	Description
time-range	Configures time range objects.

show tls-proxy

To display TLS proxy and session information, use the **show tls-proxy** command in global configuration mode.

show tls-proxy [*tls_name* | [**session** [**host** *host_addr* | **detail** [**cert-dump**] | **count** | **statistics**]]]

Syntax Description

cert-dump	Dumps the local dynamic certificate. Output is a hex dump of the LDC.
count	Shows only the session counters.
detail [**cert-dump**]	Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC. Add the **cert-dump** keyword to get a hexadecimal dump of the local dynamic certificate (LDC). You can also use these keywords with the **host** option.
host *host_addr*	Specifies the IPv4 or IPv6 address of a particular host to show the associated sessions associated.
session	Shows active TLS proxy sessions.
statistics	Shows statistics for monitoring and managing TLS sessions.
tls_name	Name of the TLS proxy to show.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was added.
8.3(1)	The **statistics** keyword was added.

Examples

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

```
ciscoasa# show tls-proxy
TLS-Proxy 'proxy': ref_cnt 1, seq#1
 Server proxy:
```

```
  Trust-point: local_ccm
 Client proxy:
  Local dynamic certificate issuer: ldc_signer
  Local dynamic certificate key-pair: phone_common
  Cipher-suite <unconfigured>
 Run-time proxies:
  Proxy 0x448b468: Class-map: skinny_ssl, Inspect: skinny
   Active sess 1, most sess 4, byte 3244
```

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

```
ciscoasa# show tls-proxy session
outside 133.9.0.211:51291 inside 195.168.2.200:2443 P:0x4491a60(proxy)
S:0x482e790 byte 3388
```

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

```
ciscoasa# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcbc10748 byte
1831704
 Client: State SSLOK  Cipher AES128-SHA Ch 0xca55efc8 TxQSize 0 LastTxLeft 0 Flags 0x1
 Server: State SSLOK  Cipher AES128-SHA Ch 0xca55efa8 TxQSize 0 LastTxLeft 0 Flags 0x9
Local Dynamic Certificate
 Status: Available
 Certificate Serial Number: 29
 Certificate Usage: General Purpose
 Public Key Type: RSA (1024 bits)
 Issuer Name:
  cn=TLS-Proxy-Signer
 Subject Name:
  cn=SEP0002B9EB0AAD
  o=Cisco Systems Inc
  c=US
 Validity Date:
  start date: 00:47:12 PDT Feb 27 2007
  end   date: 00:47:12 PDT Feb 27 2008
 Associated Trustpoints:
```

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

```
ciscoasa# show tls-proxy session stastics
TLS Proxy Sessions (Established: 600)
    Mobility:                                          0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
    SIP:                                               2
    SCCP:                                             20
    DIAMETER:                                        200
Total TLS Proxy Sessions
    Established:                                     822
    Platform Limit:                                 1000
```

Related Commands

Command	Description
client	Defines a cipher suite and sets the local dynamic certificate issuer or keypair.
ctl-provider	Defines a CTL provider instance and enters provider configuration mode.
show running-config tls-proxy	Shows running configuration of all or specified TLS proxies.

Command	Description
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show track

To display information about object tracked by the security-level agreement (SLA) tracking process, use the **show track** command in user EXEC mode.

show track [*track-id*]

Syntax Description

track-id	A tracking entry object ID number, from 1 to 500.

Command Default

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

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.

Examples

The following is sample output from the **show track** command:

```
ciscoasa(config)# show track
Track 5
 Response Time Reporter 124 reachability
 Reachability is UP
 2 changes, last change 03:41:16
 Latest operation return code: OK
 Tracked by:
  STATIC-IP-ROUTING 0
```

Related Commands

Command	Description
show running-config track	Displays the **track rtr** commands in the running configuration.
track rtr	Creates a tracking entry to poll the SLA.

show traffic

To display interface transmit and receive activity, use the **show traffic** command in privileged EXEC mode.

show traffic

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	Output for the ASA 5550 was added.
9.3(1)	Output for aggregated traffic on physical interfaces was added.
9.5(2)	SCTP and SCTP inspection were added to the detailed output.

Usage Guidelines

The **show traffic** command lists the number of packets and bytes moving through each interface since the last **show traffic** command was entered or since the ASA came online. The number of seconds is the duration the ASA has been online since the last reboot, unless the **clear traffic** command was entered since the last reboot. If this is the case, then the number of seconds is the duration since that command was entered.

For the ASA 5550, the **show traffic** command also shows the aggregated throughput per slot. Because the ASA 5550 requires traffic to be evenly distributed across slots for maximum throughput, this output helps you determine if the traffic is distributed evenly.

To show aggregated traffic on physical interfaces, you must first enter the **sysopt traffic detailed-statistics** command to turn on this feature.

Examples

The following is sample output from the **show traffic** command:

```
ciscoasa# show traffic
outside:        received (in 102.080 secs):               2048 packets 204295 bytes
          20 pkts/sec 2001 bytes/sec        transmitted (in 102.080 secs):
2048 packets 204056 bytes              20 pkts/sec 1998 bytes/secEthernet0:       received
 (in 102.080 secs):               2049 packets 233027 bytes                20 pkts/sec
2282 bytes/sec        transmitted (in 102.080 secs):               2048 packets 232750
bytes               20 pkts/sec 2280 bytes/sec
```

For the ASA 5550, the following text is displayed at the end:

```
----------------------------------------
        Per Slot Throughput Profile
----------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|****************
    Slot 1:       3149  50%|****************
  Bytes-per-second profile:
    Slot 0:     427044  50%|****************
    Slot 1:     427094  50%|****************
```

The following example shows the added output for aggregated traffic on physical interfaces:

```
IP packet size distribution (values listed in percentages)
Total Packets = 1278:
      32    64    96   128   192   256   512
    00.0  43.5  10.4  10.1  26.1  01.4  03.6

    1024  1536  2048  4096  8192  9216
    03.6  06.6  00.0  00.0  00.0  00.0

Protocol         Total    Conns   Packets   Bytes  Packets    Total
--------         Conns     /Sec     /Conn    /Pkt     /Sec  Packets
```

SCTP 0 0.0 0 0 0.0 0

```
SCTP-inspected        0      0.0       N/A     N/A      0.0        0
TCP                   8      0.2        98     215     26.8     1279
TCP-inspected         0      0.0       N/A     N/A      0.0        0
UDP                   3      0.0         0      90      0.0        2
UDP-inspected         5      0.0         1     189      0.0       56
ICMP                  0      0.0         1      98      0.0        2
ESP                   0      0.0       N/A     N/A      0.0        0
IP                    0      0.0       N/A     N/A      0.0        0
Total:               16      0.2        22     207     26.8     1433

Last clearing of statistics: Never
```

Related Commands

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