



show tcpstat through show traffic Commands

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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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 59-1 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.
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.

Table 59-1 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 ASA:

```
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
```

show tcpstat

```
tcp bad checksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

Related Commands

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

show tech-support

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	The detail and file keywords were added.
7.2(1)	The output 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.

Usage Guidelines

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

Examples

The following example shows how to display information that is used for technical support analysis. The output was shortened to begin with output from the **show module** command.

```
hostname# show tech-support | beg show module
```

```
----- show module -----
```

```
Mod Card Type
```

```
Model
```

```
Serial No.
```

```

-----
 0 ASA 5585-X Security Services Processor-10 wi ASA5585-SSP-10      JAD1626056J
-----
Mod MAC Address Range                Hw Version  Fw Version  Sw Version
-----
 0 a493.4c43.0d68 to a493.4c43.0d73  2.0         2.0(13)0    100.8(0)229
-----
Mod SSP Application Name              Status      SSP Application Version
-----

Mod Status          Data Plane Status  Compatibility
-----
 0 Up Sys           Not Applicable
-----

```

```

----- show environment -----

```

Cooling Fans:

```

-----

```

Power Supplies:

```

-----

```

Left Slot (PS0): 6900 RPM - OK (Power Supply Fan)
 Right Slot (PS1): 7200 RPM - OK (Fan Module Fan)

Power Supplies:

```

-----

```

Power Supply Unit Redundancy: N/A

Temperature:

```

-----

```

Left Slot (PS0): 30 C - OK (Power Supply Temperature)
 Right Slot (PS1): 31 C - OK (Fan Module Temperature)

Cooling Fans:

```

-----

```

Left Slot (PS0): 6900 RPM - OK (Power Supply Fan)
 Right Slot (PS1): 7100 RPM - OK (Fan Module Fan)

Temperature:

```

-----

```

Processors:

```

-----

```

Processor 1: 47.0 C - OK (CPU1 Core Temperature)

Chassis:

```

-----

```

Ambient 1: 31.5 C - OK (Chassis Front Temperature)
 Ambient 2: 37.5 C - OK (Chassis Back Temperature)
 Ambient 3: 31.25 C - OK (CPU1 Front Temperature)
 Ambient 4: 32.0 C - OK (CPU1 Back Temperature)

IO Hub:

```

-----

```

Circuit Die: 49.0 C - OK (Circuit Die Temperature)

Power Supplies:

```

-----

```

Left Slot (PS0): 30 C - OK (Power Supply Temperature)
 Right Slot (PS1): 31 C - OK (Fan Module Temperature)

Voltage:

```

-----
Channel 1: 3.325 V - (3.3V (U142 VX1))
Channel 2: 1.496 V - (1.5V (U142 VX2))
Channel 3: 1.048 V - (1.05V (U142 VX3))
Channel 4: 3.337 V - (3.3V_STDBY (U142 VP1))
Channel 5: 11.665 V - (12V (U142 VP2))
Channel 6: 4.950 V - (5.0V (U142 VP3))
Channel 7: 6.853 V - (7.0V (U142 VP4))
Channel 8: 9.616 V - (IBV (U142 VH))
Channel 9: 1.046 V - (1.05VB (U209 VX2))
Channel 10: 1.213 V - (1.2V (U209 VX3))
Channel 11: 1.110 V - (1.1V (U209 VX4))
Channel 12: 1.006 V - (1.0V (U209 VX5))
Channel 13: 3.335 V - (3.3V STDBY (U209 VP1))
Channel 14: 2.499 V - (2.5V (U209 VP2))
Channel 15: 1.803 V - (1.8V (U209 VP3))
Channel 16: 1.894 V - (1.9V (U209 VP4))
Channel 17: 9.611 V - (IBV (U209 VH))
Channel 18: 2.048 V - (VTT CPU0 (U83 VX2))
Channel 19: 0.000 V - (VTT CPU1 (U83 VX3))
Channel 20: 2.048 V - (VCC CPU0 (U83 VX4))
Channel 21: 1.772 V - (VCC CPU1 (U83 VX5))
Channel 22: 1.516 V - (1.5VA (U83 VP1))
Channel 23: 0.000 V - (1.5VB (U83 VP2))
Channel 24: 8.937 V - (IBV (U83 VH))

----- show memory -----

Free memory:      4927975152 bytes (76%)
Used memory:      1514475792 bytes (24%)
-----
Total memory:      6442450944 bytes (100%)

----- show conn count -----

0 in use, 0 most used

----- show xlate count -----

0 in use, 0 most used

----- show vpn-sessiondb summary -----

No sessions to display.

----- show blocks -----

SIZE    MAX    LOW    CNT
  0    1450   1450   1450
  4     100     99     99
 80    1000   1000   1000

----- show memory detail -----

Free memory:      276580360 bytes (52%)
Used memory:
  Allocated memory in use:      67352568 bytes (13%)
  Reserved memory:      192937984 bytes (36%)
-----
Total memory:      536870912 bytes (100%)

Least free memory:      276397760 bytes (51%)

```

Most used memory: 260473152 bytes (49%)

MEMPOOL_DMA POOL STATS:

```
Non-mmapped bytes allocated = 40779776
Number of free chunks       = 66
Number of mmaped regions    = 0
Mmapped bytes allocated     = 0
Max memory footprint        = 40779776
Keepcost                    = 10852432
Max contiguous free mem     = 10852432
Allocated memory in use     = 29908112
Free memory                  = 10871664
```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
48	1	48**
256	64	18944
10852432	1	10852432*

* - top most releasable chunk.

** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
112	1	112
232	1	232
248	1	248
256	1	256
1024	64	65536
2048	3	6144
8192	1	8192
16384	3	49152
24576	2	49152
32768	3	98304
49152	1	49152
65536	3	196608
98304	3	294912
131072	1	131072
196608	3	589824
262144	2	524288
393216	1	393216
786432	1	786432
1048576	2	2097152
1572864	1	1572864
2097152	2	4194304
3145728	1	3145728
12582912	1	12582912

MEMPOOL_GLOBAL_SHARED POOL STATS:

```
Non-mmapped bytes allocated = 343932928
Number of free chunks       = 119
Number of mmaped regions    = 0
Mmapped bytes allocated     = 0
Max memory footprint        = 343932928
Keepcost                    = 276525880
```



```

Max contiguous free mem      =    276525880
Allocated memory in use     =    67352568
Free memory                  =    276580360

```

----- fragmented memory statistics -----

fragment size (bytes)	count	total (bytes)
16	37	592
24	37	888
32	21	672
40	18	720
48	1	48**
56	1	56
184	1	184
2048	1	3048
32768	1	33616
276525880	1	276525880*

* - top most releasable chunk.

** - contiguous memory on top of heap.

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
48	544	26112
56	2438	136528
64	6806	435584
72	524	37728
80	1071	85680
88	242	21296
96	240	23040
104	2258	234832
112	66	7392
120	157	18840
128	162	20736
136	8	1088
144	11	1584
152	457	69464
160	387	61920
168	151	25368
176	204	35904
184	391	71944
192	20	3840
208	112	23296
216	1	216
224	27	6048
232	12	2784
240	44	10560
248	41	10168
256	321	82176
384	451	173184
512	253	129536
768	86	66048
1024	97	99328
1536	35	53760
2048	367	751616
3072	84	258048
4096	51	208896
6144	13	79872

8192	35	286720
12288	34	417792
16384	127	2080768
24576	16	393216
32768	35	1146880
49152	10	491520
65536	126	8257536
98304	4	393216
131072	21	2752512
196608	7	1376256
262144	7	1835008
393216	2	786432
524288	14	7340032
786432	1	786432
1048576	2	2097152
1572864	1	1572864
2097152	1	2097152
3145728	1	3145728
4194304	1	4194304
8388608	2	16777216

Summary for all pools:

```

Non-mmapped bytes allocated = 384712704
Number of free chunks       = 185
Number of mmapped regions   = 0
Mmapped bytes allocated     = 0
Max memory footprint        = 384712704
Keepcost                    = 287378312
Allocated memory in use     = 97260680
Free memory                  = 287452024

```

----- show memory top-usage -----

MEMPOOL_DMA pool binsize allocated byte totals:

----- allocated memory statistics -----

fragment size (bytes)	count	total (bytes)
12582912	1	12582912
2097152	2	4194304
3145728	1	3145728
1048576	2	2097152
1572864	1	1572864
786432	1	786432
196608	3	589824
262144	2	524288
393216	1	393216
98304	3	294912

----- Binsize PC top usage -----

Binsize: 12582912 total (bytes): 12582912

pc = 0x805ada0, size = 12960071 , count = 1

Binsize: 2097152 total (bytes): 4194304

pc = 0x805ada0, size = 5758350 , count = 2

Binsize: 3145728 total (bytes): 3145728

```

pc = 0x987071c, size = 3178567 , count = 1

Binsize: 1048576                total (bytes): 2097152

pc = 0x805ada0, size = 2309774 , count = 2

Binsize: 1572864                total (bytes): 1572864

pc = 0x805ada0, size = 1740871 , count = 1

Binsize: 786432                 total (bytes): 786432

pc = 0x805ada0, size = 915271 , count = 1

Binsize: 196608                 total (bytes): 589824

pc = 0x805ada0, size = 484622 , count = 2
pc = 0x80567f1, size = 259271 , count = 1

Binsize: 262144                 total (bytes): 524288

pc = 0x805ada0, size = 352071 , count = 1
pc = 0x80567f1, size = 310471 , count = 1

Binsize: 393216                 total (bytes): 393216

pc = 0x805ada0, size = 505671 , count = 1

Binsize: 98304                  total (bytes): 294912

pc = 0x805ada0, size = 129671 , count = 1
pc = 0x80567f1, size = 227342 , count = 2

MEMPOOL_GLOBAL_SHARED pool binsize allocated byte totals:

----- allocated memory statistics -----

fragment size      count      total
  (bytes)                (bytes)
-----
      8388608           2      16777216
         65536        126      8257536
        524288         14      7340032
       4194304          1      4194304
       3145728          1      3145728
        131072         21      2752512
        1048576          2      2097152
        2097152          1      2097152
         16384        127      2080768
        262144          7      1835008

----- Binsize PC top usage -----

Binsize: 8388608                total (bytes): 16777216

pc = 0x825b333, size = 16777216 , count = 2

Binsize: 65536                  total (bytes): 8257536

pc = 0x916e48d, size = 7531232 , count = 107
pc = 0x982de33, size = 263056 , count = 4
pc = 0x982db72, size = 324956 , count = 4

```

```

pc = 0x82d9092, size = 65536 , count = 1
pc = 0x819b8f9, size = 77824 , count = 1
pc = 0x819b65e, size = 77824 , count = 1
pc = 0x9334871, size = 65536 , count = 1
pc = 0x8a01e5a, size = 65536 , count = 1
pc = 0x8a109f0, size = 65536 , count = 1
pc = 0x9162fb0, size = 163968 , count = 2
pc = 0x8f13da8, size = 66048 , count = 1
pc = 0x8056c11, size = 66528 , count = 1
pc = 0x8056bf5, size = 66528 , count = 1

Binsize: 524288 total (bytes): 7340032

pc = 0x8a9f8eb, size = 643264 , count = 1
pc = 0x982db72, size = 5325112 , count = 8
pc = 0x807bcb4, size = 524312 , count = 1
pc = 0x821944f, size = 1282600 , count = 2
pc = 0x9187575, size = 524312 , count = 1
pc = 0x8056a14, size = 524352 , count = 1

Binsize: 4194304 total (bytes): 4194304

pc = 0x8cc1f27, size = 5242924 , count = 1

Binsize: 3145728 total (bytes): 3145728

pc = 0x821944f, size = 3698788 , count = 1

Binsize: 131072 total (bytes): 2752512

pc = 0x9137bc4, size = 163904 , count = 1
pc = 0x806e421, size = 393216 , count = 3
pc = 0x8f3f649, size = 154136 , count = 1
pc = 0x911894b, size = 131072 , count = 1
pc = 0x89f3fd0, size = 141212 , count = 1
pc = 0x982de33, size = 593580 , count = 4
pc = 0x8167e2b, size = 160864 , count = 1
pc = 0x982db72, size = 983250 , count = 6
pc = 0x9162fb0, size = 327808 , count = 2
pc = 0x806e024, size = 184800 , count = 1

Binsize: 1048576 total (bytes): 2097152

pc = 0x982de33, size = 1081507 , count = 1
pc = 0x821944f, size = 1120100 , count = 1

Binsize: 2097152 total (bytes): 2097152

pc = 0x8aa1252, size = 2097152 , count = 1

Binsize: 16384 total (bytes): 2080768

pc = 0x806e421, size = 1474560 , count = 90
pc = 0x982de33, size = 135545 , count = 7
pc = 0x9173a77, size = 36928 , count = 2
pc = 0x88a6fec, size = 163840 , count = 10
pc = 0x8f3f649, size = 24160 , count = 1
pc = 0x982db72, size = 96195 , count = 5
pc = 0x8a765c0, size = 17408 , count = 1
pc = 0x92cb71b, size = 17388 , count = 1
pc = 0x982dbee, size = 119925 , count = 7
pc = 0x879defa, size = 19456 , count = 1
pc = 0x8ebd433, size = 16432 , count = 1
pc = 0x8ebd415, size = 16432 , count = 1

```

```

Binsize: 262144                      total (bytes): 1835008

pc = 0x982db72, size = 1573315 , count = 5
pc = 0x982de33, size = 580878 , count = 2

----- show vlan -----

64, 66, 70-72, 80-82, 142, 151, 950-951, 960-961

```

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.
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 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	•	•	•	—	—

Release	Modification
8.3(1)	This command was introduced.

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:

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

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

The display output shows the following:

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

The 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:

```
hostname# show threat-detection rate
```

	Average (eps)	Current (eps)	Trigger	Total events
10-min ACL drop:	0	0	0	16
1-hour ACL drop:	0	0	0	112
1-hour SYN attck:	5	0	2	21438
10-min Scanning:	0	0	29	193
1-hour Scanning:	106	0	10	384776
1-hour Bad pkts:	76	0	2	274690
10-min Firewall:	0	0	3	22
1-hour Firewall:	76	0	2	274844
10-min DoS attck:	0	0	0	6
1-hour DoS attck:	0	0	0	42
10-min Interface:	0	0	0	204

■ show threat-detection rate

```
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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Examples

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

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

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

show threat-detection shun

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

show threat-detection shun

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

show threat-detection statistics host

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

The display output shows the following:

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

The 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:

```
hostname# show threat-detection statistics host

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

Table 59-2 shows each field description.

Table 59-2 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.

Table 59-2 *show threat-detection statistics host Fields (continued)*

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

Table 59-2 *show threat-detection statistics host Fields (continued)*

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

Related Commands

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

show threat-detection statistics port

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

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

Syntax Description

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

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

The display output shows the following:

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

The 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:

```
hostname# show threat-detection statistics port
```

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

Table 59-2 shows each field description.

Table 59-3 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

Table 59-3 *show threat-detection statistics port Fields (continued)*

Field	Description
Trigger	Shows the number of times the dropped packet rate limits were exceeded. For valid traffic identified in the sent and received bytes and packets rows, this value is always 0, because there are no rate limits to trigger for valid traffic.
Total events	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.
<i>port_number/port_name</i>	Shows the port number and name where the packet or byte was sent, received, or dropped.
tot-ses	Shows the total number of sessions for this port.
act-ses	Shows the total number of active sessions that the port is currently involved in.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the port.
Sent pkts	Shows the number of successful packets sent from the port.
Sent drop	Shows the number of packets sent from the port that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the port.
Recv pkts	Shows the number of successful packets received by the port.
Recv drop	Shows the number of packets received by the port that were dropped because they were part of a scanning attack.

Related Commands

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

show threat-detection statistics protocol

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

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

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

Defaults No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

The display output shows the following:

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

The 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:

```
hostname# show threat-detection statistics protocol
```

```

                                Average(eps)   Current(eps) Trigger      Total events
ICMP: tot-ses:0 act-ses:0
  1-hour Sent byte:                0             0         0           1000
  8-hour Sent byte:                0             2         0           1000
 24-hour Sent byte:                0             0         0           1000
  1-hour Sent pkts:                0             0         0             10
  8-hour Sent pkts:                0             0         0             10
 24-hour Sent pkts:                0             0         0             10
```

Table 59-2 shows each field description.

Table 59-4 *show threat-detection statistics protocol Fields*

Field	Description
Average(evs)	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(evs)	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(evs) 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.
<i>protocol_number/ protocol_name</i>	Shows the protocol number and name where the packet or byte was sent, received, or dropped.
tot-ses	Not currently used.
act-ses	Not currently used.
20-min, 1-hour, 8-hour, and 24-hour	Shows statistics for these fixed rate intervals.
Sent byte	Shows the number of successful bytes sent from the protocol.
Sent pkts	Shows the number of successful packets sent from the protocol.
Sent drop	Shows the number of packets sent from the protocol that were dropped because they were part of a scanning attack.
Recv byte	Shows the number of successful bytes received by the protocol.

Table 59-4 *show threat-detection statistics protocol Fields (continued)*

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

Related Commands

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

show threat-detection statistics top

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

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

Syntax Description

access-list	(Optional) Shows the top 10 ACEs that 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 <i>min_display_rate</i>	(Optional) Limits the display to statistics that exceed the minimum display rate in events per second. You can set the <i>min_display_rate</i> between 0 and 2147483647.
port-protocol	(Optional) Shows the top 10 combined statistics of TCP/UDP port and IP protocol types. TCP (protocol 6) and UDP (protocol 17) are not included in the display for IP protocols; TCP and UDP ports are, however, included in the display for ports. If you only enable statistics for one of these types, port or protocol, then you will only view the enabled statistics.
rate-1	(Optional) Shows the statistics for the smallest fixed rate intervals available in the display. For example, if the display shows statistics for the last 1 hour, 8 hours, and 24 hours, then when you use the rate-1 keyword, the 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.

Defaults

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

Command Modes

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

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

Command History

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

Usage Guidelines

The display output shows the following:

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

The 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:

```
hostname# show threat-detection statistics top access-list
```

Top	Average(eps)	Current(eps)	Trigger	Total events
1-hour ACL hits:				
100/3[0]	173	0	0	623488
200/2[1]	43	0	0	156786
100/1[2]	43	0	0	156786

```

8-hour ACL hits:
      100/3 [0]          21          1298          0          623488
      200/2 [1]           5           326          0          156786
      100/1 [2]           5           326          0          156786

```

Table 59-2 shows each field description.

Table 59-5 *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 than 10 ACEs might be listed.
Average(eps)	Shows the average rate in events/sec over each time period. The security appliance stores the count at the end of each burst period, for a total of 30 completed burst intervals. The unfinished burst interval presently occurring is not included in the average rate. For example, if the average rate interval is 20 minutes, then the burst interval is 20 seconds. If the last burst interval was from 3:00:00 to 3:00:20, and you use the show command at 3:00:25, then the last 5 seconds are not included in the output. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the 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 denials using the show threat-detection rate access-list command.
Total events	Shows the total number of events over each rate interval. The unfinished burst interval presently occurring is not included in the total events. The only exception to this rule is if the number of events in the unfinished burst interval already exceeds the number of events in the oldest burst interval (#1 of 30) when calculating the total events. In that case, the 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.
1-hour, 8-hour	Shows statistics for these fixed rate intervals.
<i>acl_name/line_number</i>	Shows the access list name and line number of the ACE that caused the denials.

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

```
hostname# show threat-detection statistics top access-list rate-1
```

show threat-detection statistics top

```

Top      Average(eps)    Current(eps) Trigger      Total events
1-hour ACL hits:
100/3[0]      173              0      0      623488
200/2[1]      43               0      0      156786
100/1[2]      43               0      0      156786

```

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

```
hostname# show threat-detection statistics top port-protocol
```

```

Top      Name      Id      Average(eps)    Current(eps) Trigger      Total events
1-hour Recv byte:
1      gopher      70      71              0      0      32345678
2      btp-clnt/dhcp 68      68              0      0      27345678
3      gopher      69      65              0      0      24345678
4      Protocol-96 * 96      63      0      0      22345678
5      Port-7314 7314      62      0      0      12845678
6      BitTorrent/trc 6969      61      0      0      12645678
7      Port-8191-65535 55      0      0      12345678
8      SMTP      366      34      0      0      3345678
9      IPinIP * 4      30      0      0      2345678
10     EIGRP * 88      23      0      0      1345678
1-hour Recv pkts:
...
...
8-hour Recv byte:
...
...
8-hour Recv pkts:
...
...
24-hour Recv byte:
...
...
24-hour Recv pkts:
...
...

```

Note: Id preceded by * denotes the Id is an IP protocol type

Table 59-6 shows each field description.

Table 59-6 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 than 10 ports/protocols might be listed.
Name	Shows the port/protocol name.
Id	Shows the port/protocol ID number. The asterisk (*) means the ID is an IP protocol number.
Average(eps)	See the description in Table 59-2 .
Current(eps)	See the description in Table 59-2 .
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.

Table 59-6 *show threat-detection statistics top port-protocol Fields (continued)*

Field	Description
Total events	See the description in Table 59-2 .
<i>Time_interval</i> Sent byte	Shows the number of successful bytes sent from the listed ports and protocols for each time period.
<i>Time_interval</i> Sent packet	Shows the number of successful packets sent from the listed ports and protocols for each time period.
<i>Time_interval</i> Sent drop	Shows the number of packets sent for each time period from the listed ports and protocols that were dropped because they were part of a scanning attack.
<i>Time_interval</i> Recv byte	Shows the number of successful bytes received by the listed ports and protocols for each time period.
<i>Time_interval</i> Recv packet	Shows the number of successful packets received by the listed ports and protocols for each time period.
<i>Time_interval</i> Recv drop	Shows the number of packets received for each time period by the listed ports and protocols that were dropped because they were part of a scanning attack.
<i>port_number/</i> <i>port_name</i>	Shows the port number and name where the packet or byte was sent, received, or dropped.
<i>protocol_number/</i> <i>protocol_name</i>	Shows the protocol number and name where the packet or byte was sent, received, or dropped.

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

```
hostname# show threat-detection statistics top host
```

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

show threat-detection statistics top

```

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 59-7 shows each field description.

Table 59-7 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 than 10 hosts might be listed.
Average(eps)	See the description in Table 59-2.
Current(eps)	See the description in Table 59-2.
Trigger	See the description in Table 59-2.
Total events	See the description in Table 59-2.
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.
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.

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

```
hostname# show threat-detection statistics top tcp-intercept
```

```

Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins   Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
-----
1   192.168.1.2:5000 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2   192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3   192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4   192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5   192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6   192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7   192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8   192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
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 59-8 shows each field description.

Table 59-8 *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.
<i>rank</i>	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
<i>server_ip:port</i>	Shows the server IP address and the port on which it is being attacked.
<i>interface</i>	Shows the interface through which the server is being attacked.
<i>avg_rate</i>	Shows the average rate of attack, in attacks per second over the sampling period
<i>current_rate</i>	Shows the current attack rate, in attacks per second.
<i>total</i>	Shows the total number of attacks.
<i>attacker_ip</i>	Shows the attacker IP address.
<i>(last_attack_time ago)</i>	Shows when the last attack occurred.

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

```
hostname# show threat-detection statistics top tcp-intercept long

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

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

```
hostname# show threat-detection statistics top tcp-intercept detail

Top 10 Protected Servers under Attack (sorted by average rate)
Monitoring Window Size: 30 mins    Sampling Interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack Time)>
-----
1    192.168.1.2:5000 inside 1877 9502 3379276 <various> Last: 10.0.0.45 (0 secs ago)
```

show threat-detection statistics top

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 59-9 shows each field description.

Table 59-9 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.
<i>rank</i>	Shows the ranking, 1 through 10, where 1 is the most attacked server, and 10 is the least attacked server.
<i>server_ip:port</i>	Shows the server IP address and the port on which it is being attacked.
<i>interface</i>	Shows the interface through which the server is being attacked.
<i>avg_rate</i>	Shows the average rate of attack, in attacks per second over the rate interval set by the threat-detection statistics tcp-intercept rate-interval command (by default, the rate interval is 30 minutes). The ASA samples the data every 30 seconds over the rate interval.
<i>current_rate</i>	Shows the current attack rate, in attacks per second.
<i>total</i>	Shows the total number of attacks.
<i>attacker_ip</i> or <various> Last: <i>attacker_ip</i>	Shows the attacker IP address. If there is more than one attacker, then “<various>” displays followed by the last attacker IP address.
(<i>last_attack_time</i> ago)	Shows when the last attack occurred.
<i>sampling data</i>	Shows all 30 sampling data values, which show the number of attacks at each interval.

Related Commands

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

show tls-proxy

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

show tls-proxy *tls_name* [**session** [**host** *host_addr* | **detail** [**cert-dump** | **count**] [**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		Shows detailed TLS proxy information including the cipher for each SSL leg and the LDC.
host <i>host_addr</i>		Specifies a particular host to show the sessions associated with.
session		Shows active TLS proxy sessions.
statistics		Shows statistics for monitoring and managing TLS sessions.
<i>tls_name</i>		Name of the TLS proxy to show.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Examples

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

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

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

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

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

```
hostname# show tls-proxy session detail
1 in use, 1 most used
outside 133.9.0.211:50433 inside 195.168.2.200:2443 P:0xcba60b60(proxy) S:0xcabc10748 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:

```
hostname# show tls-proxy session statics
  TLS Proxy Sessions (Established: 600)
    Mobility:                200
    UC-IME:                  400

  Per-Session Licensed TLS Proxy Sessions
  (Established: 222, License Limit: 250)
    SIP:                     2
    SCCP:                    20
    Phone Proxy:             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	Shows running configuration of all or specified TLS proxies.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

show track

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

show track [*track-id*]

Syntax Description

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:

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

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

```
hostname(config)# show track
```

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

Related Commands

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

show traffic

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

show traffic

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Release	Modification
7.2(1)	Output for the ASA 5550 was added.

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.

Examples The following is sample 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, 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.

