CHAPTER 13

show tcpstat コマンド～ show traffic コマンド

show tcpstat

ASAの TCP スタックおよびASAで終端している TCP 接続のステータスを(デバッグのために)表示するには、特権 EXEC モードで **show tcpstat** コマンドを使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

show tcpstat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよびASAで終端している TCP 接続のステータスを表示できます。表 28 に、表示される TCP 統計情報の説明を示します。

表 13-1　show tcpstat コマンドの TCP 統計情報

統計	説明
tcb_cnt	TCP ユーザの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザ認可で使用されます。
tcp_xmt pkts	TCP スタックが送信したパケットの数。
tcp_rcv good pkts	TCP スタックが受信した正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	チェックサムに誤りがあった受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザの数。
tcp user hash add dup	新しい TCP ユーザをハッシュ テーブルに追加しようとしたとき、そのユーザがすでにテーブル内に存在していた回数。

表 13-1　　show tcpstat コマンドの TCP 統計情報(続き)

統計	説明
tcp user srch hash hit	検索時にハッシュ テーブル内で TCP ユーザが検出された回数。
tcp user srch hash miss	検索時にハッシュ テーブル内で TCP ユーザが検出されなかった回数。
tcp user hash delete	TCP ユーザがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザを削除しようとしたとき、そのユーザがハッシュ テーブル内で検出されなかった回数。
lip	TCP ユーザのローカル IP アドレス。
fip	TCP ユーザの外部 IP アドレス。
lp	TCP ユーザのローカル ポート。
fp	TCP ユーザの外部ポート。
st	TCP ユーザの状態(RFC 793 を参照)。表示される値は次のとおりです。 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	TCP ユーザの再送信キューの長さ。
inqlen	TCP ユーザの入力キューの長さ。
tw_timer	TCP ユーザの time_wait タイマーの値(ミリ秒)。
to_timer	TCP ユーザの非アクティビティ タイムアウト タイマーの値(ミリ秒)。
cl_timer	TCP ユーザのクローズ要求タイマーの値(ミリ秒)。
per_timer	TCP ユーザの持続タイマーの値(ミリ秒)。
rt_timer	TCP ユーザの再送信タイマーの値(ミリ秒)。
tries	TCP ユーザの再送信回数。

例

次に、ASAの TCP スタックのステータスを表示する例を示します。

```
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
```

関連コマンド

コマンド	説明
show conn	使用されている接続と使用可能な接続を表示します。

show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

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

構文の説明

detail	(任意)詳細情報を表示します。
file	(任意)コマンドの出力をファイルに書き込みます。ファイル システムのタイプは次のとおりです。disk0:、disk1:、ftp:、scp:、smb:、および tftp:。
no-config	(任意)実行コンフィギュレーションの出力を除外します。
performance	(オプション)パフォーマンス情報を表示します。
vsn	(オプション)ファイルにリダイレクトされる追加の ASA1000V ポリシー エージェントのテクニカル サポート情報を含めます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	• Yes

コマンド履歴

リリース	変更内容
7.0(1)	**detail** キーワードおよび **file** キーワードが追加されました。
7.2(1)	出力が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。
9.1(2)	出力が拡張され、**show environment** コマンドの情報が含まれるようになりました。
9.1(3)	出力が拡張され、**show memory detail**、**show memory top-usage**、および **show vlan** コマンドの情報が含まれるようになりました。
9.2(1)	**show memory detail**、**show cpu detail**、**show blocks queue history core-local**、**show asp drop**、**show asp event dp-cp**、**show cpu usage history** および **show traffic summary** コマンドからの情報を含むように出力が拡張されました。**show kernel cgroup-controller detail** コマンドからの出力は削除されました。**performance** および **vsn** キーワードが追加されました。
9.2(1)	出力が拡張され、**show vlan** コマンドの情報が含まれるようになりました。

リリース	変更内容
9.1(7)/9.3(1)	**show tech-support** コマンドに **show resource usage count all 1** の出力が含まれるようになりました。これには、xlate、conn、inspect、syslog などに関する情報が含まれます。この情報は、パフォーマンスに関する問題を診断するために役立ちます。
9.3(2)	**show route-summary** コマンドの出力が **show tech-support detail** コマンドに追加されました。
9.4(1)	**show tech-support** コマンドの出力には、生成された syslog の最新 50 行が含まれます。これらの結果を表示できるようにするには、**logging buffer** コマンドをイネーブルにする必要があります。
9.1(7)/9.4(3)/9.5(2)	**show tech support** コマンドは現在次のとおりです。 • **dir all-filesystems** の出力が含まれます。この出力は次の場合に役立つことがあります。 – SSL VPN コンフィギュレーション:必要なリソースが ASA にあるかどうかを確認します。 – クラッシュ:クラッシュ ファイルの日付のタイムスタンプと存在を確認します。 • **show kernel cgroup-controller detail** の出力の削除:このコマンド出力は **show tech-support detail** の出力内に残されます。
9.7.(1)	**show tech-support** コマンドは、次の変更が加えられ更新されました。 • クラッシュしたスレッドからの **thread name**、**registry content**、**timestamp**、**traceback** などの crashinfo 統計情報を含むように出力が拡張されました。**Saved crash** のタイムスタンプからの出力は削除されました。 • **show ipsec stats**、**show crypto ikev1 stats** および **show crypto ikev2 stats** コマンドを含むように出力が拡張されました。これらのコマンドは、トラブルシューティングを目的として、VPN 統計情報を収集するために使用されます。 • **show tech-support** コマンドに、**show vm** の出力が含まれるようになりました。これは、ASAv が現在稼働しているハイパーバイザーを判別します。この情報は、仮想プラットフォーム上で複数の自動化されたチェックを実行するために役立ちます。 • **show tech-support** コマンドに **show module detail** コマンドが含まれるようになりました。このコマンドは、複数のモジュールに関する情報を提供するため、さまざまな接続およびステータスの問題のトラブルシューティングに役立ちます。

使用上のガイドライン

show tech-support コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。テクニカル サポート アナリストは、このコマンドと各種 **show** コマンドの出力を組み合わせてさまざまな情報を入手します。

例

次に、テクニカル サポート分析に使用される情報を表示する例を示します。出力が、**show module** コマンドの出力で始まるように短縮されています。

```
ciscoasa# 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 asp drop ------------------
Frame drop:
  Flow is denied by configured rule (acl-drop)                           290272
```

```
  Slowpath security checks failed (sp-security-failed)                    22489
  Interface is down (interface-down)                                         49
Last clearing: Never
Flow drop:
Last clearing: Never

------------------ show asp event dp-cp ------------------
DP-CP EVENT QUEUE                   QUEUE-LEN  HIGH-WATER
Punt Event Queue                            0           1
Identity-Traffic Event Queue                0           1
General Event Queue                         0           2
Syslog Event Queue                          0           3
Non-Blocking Event Queue                    0          22
Midpath High Event Queue                    0           0
Midpath Norm Event Queue                    0           1
SRTP Event Queue                            0           0
HA Event Queue                              0           3
Threat-Detection Event Queue                0           0
ARP Event Queue                             0          10
IDFW Event Queue                            0           0
CXSC Event Queue                            0           0

EVENT-TYPE          ALLOC ALLOC-FAIL ENQUEUED ENQ-FAIL  RETIRED 15SEC-RATE
punt                18079          0    18079        0    18079           0
  inspect-gtp       18079          0    18079        0    18079           0
drop-flow             0            0    36158        0    36158           0
midpath-norm          9            0        9        0        9           0
adj-absent          18079          0    18079        0    18079           0
arp-in            7683820          0  7683820        0  7683820           0
identity-traffic       16          0       16        0       16           0
syslog             117503          0   117503        0   117503           0
scheduler              89          0       89        0       89           0
ha-msg           48812863          0 48812863        0 48812863           5

------------------ show blocks queue history core-local ------------------

History buffer memory usage: 3744 bytes (default)
History analysis time limit: 100 msec

------------------ show blocks core ------------------
CORE  LIMIT  ALLOC   HIGH    CNT       FAILED
   0  24576     24     25   1111            0
   1  24576   4425   6155    899            0
   2  24576   2045   2873    743            0
   3  24576   3129   4648    817            0
   4  24576     18     18   1994            0
   5  24576    338    936   1412            0
   6  24576     40     44   2011            0
   7  24576    124    129   1155            0

------------------ show cpu detail ------------------

Break down of per-core data path versus control point cpu usage:
Core         5 sec            1 min            5 min
Core 0       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 1       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 2       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 3       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 4       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 5       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 6       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)
Core 7       0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)  0.0 (0.0 + 0.0)

Current control point elapsed versus the maximum control point elapsed for:
```

```
      5 seconds = 66.7%; 1 minute: 66.7%; 5 minutes: 66.7%
CPU utilization of external processes for:
      5 seconds = 0.2%; 1 minute: 0.0%; 5 minutes: 0.0%

Total CPU utilization for:
      5 seconds = 0.3%; 1 minute: 0.1%; 5 minutes: 0.1%

------------------ show memory detail ------------------
Free memory:                    10213725472 bytes (79%)
Used memory:
     Allocated memory in use:      789891808 bytes ( 6%)
     Reserved memory:             1881284608 bytes (15%)
-----------------------------   ------------------
Total memory:                   12884901888 bytes (100%)

Least free memory:      10213420912 bytes (79%)
Most used memory:        2671480976 bytes (21%)

MEMPOOL_DMA_ALT1 POOL STATS:

Non-mmapped bytes allocated =    291766272
Number of free chunks       =            1
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    291766272
Keepcost                    =    263907584
Max contiguous free mem     =    263907584
Allocated memory in use     =     27858592
Free memory                 =    263907680

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

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          96             1             96**
    263907584            1      263907584*

*  - top most releasable chunk.
** - contiguous memory on top of heap.


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

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
         8192            16          131072
     12582912             1       12582912

MEMPOOL_DMA POOL STATS:

Non-mmapped bytes allocated =    291766272
Number of free chunks       =          131
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =    291766272
Keepcost                    =    252590992
Max contiguous free mem     =    252590992
Allocated memory in use     =     39118960
Free memory                 =    252647312

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

```
fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          96             1             96**
         256            64          20480
         384            32          15360
         512            33          20208
   252590992             1      252590992*

*  - top most releasable chunk.
** - contiguous memory on top of heap.

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

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          96             1             96
         144             2            288
         256             2            512
         384             3           1152
         512             3           1536
        1024           128         131072
        2048             1           2048
        8192             5          40960
       12288            25         307200
       16384             1          16384
       32768             2          65536
       65536             1          65536
       98304             2         196608
      131072             3         393216
      196608             5         983040
      262144             3         786432
      393216             1         393216
      524288             2        1048576
      786432             2        1572864
     1048576             1        1048576
     1572864             2        3145728
     2097152             2        4194304
     3145728             2        6291456
    12582912             1       12582912

MEMPOOL_GLOBAL_SHARED POOL STATS:

Non-mmapped bytes allocated =  11003617280
Number of free chunks       =          492
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
Max memory footprint        =  11003617280
Keepcost                    =  10213402128
Max contiguous free mem     =  10213402128
Allocated memory in use     =    789891808
Free memory                 =  10213725472

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

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
          32           201           6432
          48           131           6288
          64           138           8832
          96             1             96**
         112             2            224
```

```
          256             5           1392
          512             1            592
         2048             1           2160
        24576            11         284784
  10213402128             1    10213402128*

*  - top most releasable chunk.
** - contiguous memory on top of heap.

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

fragment size       count          total
    (bytes)                        (bytes)
---------------  ----------  --------------
           80          1485         118800
           96          8525         818400
          112          3287         368144
          128          1867         238976
          144         10842        1561248
          160           876         140160
          176           476          83776
          192           448          86016
          208           795         165360
          224          1130         253120
          240           191          45840
          256          2733         699648
          384           415         159360
          512          1225         627200
          768           869         667392
         1024          1507        1543168
         1536          5345        8209920
         2048           329         673792
         3072           186         571392
         4096          5001       20484096
         6144            58         356352
         8192           349        2859008
        12288            94        1155072
        16384            85        1392640
        24576            17         417792
        32768           172        5636096
        49152            38        1867776
        65536           172       11272192
        98304            44        4325376
       131072            41        5373952
       196608            36        7077888
       262144            40       10485760
       393216            20        7864320
       524288            15        7864320
       786432            50       39321600
      1048576            32       33554432
      1572864             1        1572864
      2097152            12       25165824
      3145728             2        6291456
      4194304             1        4194304
      6291456             1        6291456
      8388608             1        8388608
     12582912             5       62914560

Summary for all pools:

Non-mmapped bytes allocated =  11587149824
Number of free chunks       =          624
Number of mmapped regions   =            0
Mmapped bytes allocated     =            0
```

```
Max memory footprint        =  11587149824
Keepcost                    =  10729900704
Allocated memory in use     =    856869360
Free memory                 =  10730280464


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

MEMPOOL_DMA pool binsize allocated byte totals:

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

 fragment size       count          total
    (bytes)                        (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 route-summary----------

IP routing table maximum-paths is 3
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
connected       0           2           0           176         576
static          0           1           0           88          288
eigrp 11        0           3000        0           324000      864000
bgp 200         2           45          0           4136        13536
  External: 47 Internal: 0 Local: 0
ospf 100        0           538         0           47344       157096
  Intra-area: 38 Inter-area: 0 External-1: 500 External-2: 0
  NSSA External-1: 0 NSSA External-2: 0
internal        7                                               288976
Total           9           3586        0           375744      1324472

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

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

関連コマンド

コマンド	説明
show clock	Syslog サーバ（PFSS）および公開キー インフラストラクチャ（PKI）プロトコルで使用されるクロックを表示します。
show conn count	使用されている接続と使用可能な接続を表示します。
show cpu	CPU の使用状況に関する情報を表示します。
show failover	接続のステータスおよびアクティブになっているASAを表示します。
show memory	物理メモリの最大量およびオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show perfmon	ASAのパフォーマンスに関する情報を表示します。
show processes	動作しているプロセスのリストを表示します。
show running-config	ASA上で現在実行されているコンフィギュレーションを表示します。
show xlate	変換スロットに関する情報を表示します。

show threat-detection memory

threat-detection statistics コマンドによりイネーブルにされる、脅威検出の詳細統計情報で使用されるメモリを表示するには、特権 EXEC モードで **show threat-detection memory** コマンドを使用します。

show threat-detection memory

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

統計情報によっては、大量のメモリを使用して、ASAのパフォーマンスに影響を与えることがあります。このコマンドを使用すると、必要に応じてコンフィギュレーションを調整できるようにメモリ使用率をモニタできます。

例

次に、**show threat-detection memory** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection statistics	脅威検出の詳細統計情報をイネーブルにします。

show threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにすると、特権 EXEC モードで **show threat-detection rate** コマンドを使用して統計情報を表示できます。

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**]

構文の説明

acl-drop	(任意)アクセス リストで拒否されたためにドロップされたパケットのレートを表示します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
bad-packet-drop	(任意)パケット形式に誤りがあって(invalid-ip-header または invalid-tcp-hdr-length など)拒否されたためにドロップされたパケットのレートを表示します。
conn-limit-drop	(任意)接続制限(システム全体のリソース制限および設定された制限の両方)を超えたためにドロップされたパケットのレートを表示します。
dos-drop	(任意)DoS 攻撃(無効な SPI やステートフル ファイアウォール チェック不合格など)を検出したためにドロップされたパケットのレートを表示します。
fw-drop	(任意)基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレートを表示します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	(任意)疑わしい ICMP パケットが検出されたためにドロップされたパケットのレートを表示します。
inspect-drop	(任意)アプリケーション インスペクションに不合格だったパケットが原因でドロップされたパケットのレート制限を表示します。
interface-drop	(任意)インターフェイスの過負荷が原因でドロップされたパケットのレート制限を表示します。
scanning-threat	(任意)スキャン攻撃が検出されたためにドロップされたパケットのレートを表示します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出(**threat-detection scanning-threat** コマンドを参照)では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	(オプション)TCP SYN 攻撃や戻りデータなしの UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレートを表示します。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 一定時間における平均レート（イベント/秒）。
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートが制限を超えた回数。
- 固定された期間におけるイベントの合計数

ASAは、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASAは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 10 分の場合、バースト間隔は 10 秒です。最後のバースト間隔が 3:00:00 から 3:00:10 までであった場合に **show** コマンドを 3:00:15 に使用すると、最後の 5 秒分の情報は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最新の 59 の完了した間隔のイベント数および未完了のバースト間隔の現在までのイベント数を合計して、合計イベント数を計算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection rate** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection scanning-threat

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにした場合は、特権 EXEC モードで **show threat-detection scanning-threat** コマンドを使用すると、攻撃者および攻撃対象と分類されたホストが表示されます。

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

構文の説明

attacker	（任意）攻撃元ホストの IP アドレスを表示します。
target	（オプション）攻撃対象ホストの IP アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	見出しテキストに「& Subnet List」を表示するように変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。
9.0	インターフェイス情報が出力に追加されました。

例

次に、**show threat-detection scanning-threat** コマンドの出力例を示します。

```
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)
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection shun	現在回避されているホストを表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection shun

threat-detection scanning-threat コマンドを使用してスキャンによる脅威の検出をイネーブルにし、攻撃元ホストを自動的に回避した場合は、特権 EXEC モードで **show threat-detection shun** コマンドを使用すると、現在回避されているホストが表示されます。

show threat-detection shun

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。
9.0	インターフェイス情報が出力に追加されました。

使用上のガイドライン

排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、**show threat-detection shun** コマンドの出力例を示します。

```
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
```

関連コマンド

コマンド	説明
clear threat-detection shun	排除対象からホストを除外します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

show threat-detection statistics host

threat-detection statistics host コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics host**コマンドを使用するとホスト統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

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

構文の説明

ip_address	(任意)特定のホストの統計情報を表示します。
mask	(任意)ホスト IP アドレスのサブネット マスクを設定します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート(イベント数/秒)
- 終了した最後のバースト間隔における現在のバースト レート(イベント数/秒)。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数(ドロップされたトラフィックの統計情報の場合に限る)
- 固定された期間におけるイベントの合計数

ASAは、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASAは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics host** コマンドの出力例を示します。

```
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
```

表 13-2 に、各フィールドの説明を示します。

表 13-2　show threat-detection statistics host のフィールド

フィールド	説明
Host	ホストの IP アドレスを表示します。
tot-ses	ホストがデータベースに追加されて以降の、このホストでの合計セッション数を表示します。
act-ses	ホストが現在関係しているアクティブなセッションの合計数を表示します。
fw-drop	ファイアウォールでのドロップ数を表示します。ファイアウォール ドロップは、基本脅威検出で追跡されたすべてのファイアウォール関連のパケット ドロップを含む組み合わせレートです。これには、アクセス リストでの拒否、不良パケット、接続制限の超過、DoS 攻撃パケット、疑わしい ICMP パケット、TCP SYN 攻撃パケット、および戻りデータなしの UDP セッション攻撃パケットなどが含まれます。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません。
insp-drop	アプリケーション インスペクションに不合格になったためにドロップされたパケット数を表示します。
null-ses	ヌル セッションの数を表示します。ヌル セッションとは、タイムアウトするまでの 30 秒以内に完了しなかった TCP SYN セッションと、セッションが開始されてから 3 秒以内にサーバからデータの送信がなかった UDP セッションです。
bad-acc	閉じられた状態のホストのポートに対する不正なアクセスの試行回数を表示します。ポートがヌル セッション状態（上記を参照）であると判定されると、ホストのポート状態は HOST_PORT_CLOSE に設定されます。そのホストのポートにアクセスしようとするクライアントはすべて、タイムアウトを待たずにすぐ不正アクセスとして分類されます。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。

表 13-2　show threat-detection statistics host のフィールド（続き）

フィールド	説明
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
20-min、1-hour、8-hour、および 24-hour	デフォルトでは、3 つのレート間隔が表示されます。**threat-detection statistics host number-of-rate** コマンドを使用すると、レート間隔の数を減らすことができます。ホスト統計情報では大量のメモリが使用されるため、レート間隔の数値をデフォルトの 3 より減らすと、メモリ使用率が軽減します。このキーワードを 1 に設定すると、最短のレート間隔統計情報だけが保持されます。値を 2 に設定すると、2 つの最短の間隔が保持されます。
Sent byte	ホストから正常に送信されたバイト数を表示します。
Sent pkts	ホストから正常に送信されたパケット数を表示します。
Sent drop	ホストから送信されたパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。
Recv byte	ホストが正常に受信したバイト数を表示します。
Recv pkts	ホストが正常に受信したパケット数を表示します。
Recv drop	ホストが受信したパケットの中で、スキャン攻撃の一部であったためにドロップされたパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics port

threat-detection statistics port コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics port** コマンドを使用すると、TCP ポートおよび UDP ポートの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

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

構文の説明

start_port[**-***end_port*]	（任意）0 ～ 65535 の間の特定のポートまたはポート範囲の統計情報を表示します。
min-display-rate *min_display_rate*	（任意）最小表示レート（毎秒あたりのイベント数）を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASAは、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASAは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics port** コマンドの出力例を示します。

```
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
```

表 13-2 に、各フィールドの説明を示します。

表 13-3　show threat-detection statistics port のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
port_number/*port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
tot-ses	このポートのセッションの合計数を表示します。
act-ses	ポートが現在関係しているアクティブなセッションの合計数を表示します。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	ポートから正常に送信されたバイト数を表示します。
Sent pkts	ポートから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、ポートから送信されたパケット数を表示します。
Recv byte	ポートが正常に受信したバイト数を表示します。
Recv pkts	ポートが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、ポートが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics protocol

threat-detection statistics protocol コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics protocol** コマンドを使用すると、IP プロトコルの統計情報が表示されます。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

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

構文の説明

protocol_number	(任意)0 ～ 255 の間の特定のプロトコル番号の統計情報を表示します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
protocol_name	(任意)特定のプロトコル名の統計情報を表示します。 • **ah** • **eigrp** • **esp** • **gre** • **icmp** • **igmp** • **igrp** • **ip** • **ipinip** • **ipsec** • **nos** • **ospf** • **pcp** • **pim** • **pptp** • **snp** • **tcp** • **udp**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート（イベント数/秒）
- 終了した最後のバースト間隔における現在のバースト レート（イベント数/秒）。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数（ドロップされたトラフィックの統計情報の場合に限る）
- 固定された期間におけるイベントの合計数

ASAは、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASAは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics protocol** コマンドの出力例を示します。

```
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
```

表 13-4 に、各フィールドの説明を示します。

表 13-4　show threat-detection statistics protocol のフィールド

フィールド	説明
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明で示された例の場合、現在レートは 3:19:30 ～ 3:20:00 のレートです。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
protocol_number/ protocol_name	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。
tot-ses	現在使用されていません。
act-ses	現在使用されていません。
20-min、1-hour、8-hour、および 24-hour	これらの固定レート間隔における統計情報を表示します。
Sent byte	プロトコルから正常に送信されたバイト数を表示します。
Sent pkts	プロトコルから正常に送信されたパケット数を表示します。
Sent drop	スキャン攻撃の一部であったためにドロップされた、プロトコルから送信されたパケット数を表示します。
Recv byte	プロトコルが正常に受信したバイト数を表示します。
Recv pkts	プロトコルが正常に受信したパケット数を表示します。
Recv drop	スキャン攻撃の一部であったためにドロップされた、プロトコルが受信したパケット数を表示します。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics host	ホストの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show threat-detection statistics top

threat-detection statistics コマンドを使用して脅威の統計情報をイネーブルにした場合は、特権 EXEC モードで **show threat-detection statistics top**コマンドを使用すると、上位 10 件の統計情報が表示されます。特定のタイプで脅威の検出の統計情報がイネーブルでない場合、このコマンドではそれらの統計情報を表示できません。脅威検出統計情報には、許可およびドロップされたトラフィック レートが表示されます。

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**]]

構文の説明

access-list	(任意)許可 ACE と拒否 ACE の両方を含む、パケットに一致する上位 10 件の ACE を表示します。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。
all	(任意)TCP 代行受信の場合、追跡されたすべてのサーバの履歴データを表示します。
detail	(任意)TCP 代行受信の場合、サンプリング データの履歴を表示します。
host	(任意)一定期間ごとに上位 10 件のホスト統計情報を表示します。 (注) 脅威の検出アルゴリズムにより、フェールオーバー リンクまたはステート リンクに使用するインターフェイスは、上位 10 のホストの 1 つとして表示される可能性があります。この現象は、フェールオーバー リンクとステート リンクの両方に 1 つのインターフェイスを使用するときに発生する可能性が高くなります。これは正常な動作であり、この IP アドレスが表示されても無視してかまいません。
long	(任意)サーバの実際の IP アドレスおよび無変換の IP アドレスとともに、統計情報の履歴をロング フォーマットで表示します。
min-display-rate *min_display_rate*	(任意)最小表示レート(毎秒あたりのイベント数)を超えた統計情報だけが表示されるように制限します。*min_display_rate* は、0 ～ 2147483647 の値に設定できます。
port-protocol	(任意)TCP/UDP ポート タイプと IP プロトコル タイプを組み合わせた上位 10 件の統計情報を表示します。TCP(プロトコル 6)と UDP(プロトコル 17)は、IP プロトコルの表示には含まれていませんが、TCP ポートと UDP ポートはポートの表示に含まれています。これらのタイプ(ポートまたはプロトコル)の 1 つの統計情報だけをイネーブルにすると、イネーブルにされた統計情報だけが表示されます。
rate-1	(任意)表示されている一定レート間隔のうち、最小のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-1** キーワードを使用すると、1 時間間隔だけがASAに表示されます。
rate-2	(任意)表示されている一定レート間隔のうち、中間のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-2** キーワードを使用すると、8 時間間隔だけがASAに表示されます。

rate-3	(任意)表示されている一定レート間隔のうち、最大のレート間隔の統計情報を表示します。たとえば、直近の 1 時間、8 時間、および 24 時間の統計情報が表示されている場合は、**rate-3** キーワードを使用すると、24 時間間隔だけがASAに表示されます。
tcp-intercept	TCP 代行受信の統計情報を表示します。表示には、攻撃を受けて保護された上位 10 サーバが含まれます。

デフォルト

イベント タイプを指定しない場合、すべてのイベントが表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。
8.2(1)	バースト レート間隔の平均レートが 60 分の 1 から 30 分の 1 に変更されました。
8.2(2)	**tcp-intercept** に **long** キーワードが追加されました。脅威イベントについては、重大度レベルが警告から通知に変更されました。脅威イベントは 5 分ごとにトリガーできます。

使用上のガイドライン

ディスプレイの出力には、次の情報が表示されます。

- 固定された期間の平均レート(イベント数/秒)
- 終了した最後のバースト間隔における現在のバースト レート(イベント数/秒)。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうの間隔
- レートを超過した回数(ドロップされたトラフィックの統計情報の場合に限る)
- 固定された期間におけるイベントの合計数

ASAは、平均レート間隔内でイベント カウントを 30 回計算します。つまり、ASAは、合計 30 回の完了バースト間隔で、各バースト期間の終わりにレートをチェックします。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。

このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔(1/30 個目)のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。

例

次に、**show threat-detection statistics top access-list** コマンドの出力例を示します。

```
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
```

表 13-5 に、各フィールドの説明を示します。

表 13-5　show threat-detection statistics top access-list のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、時間内の ACE のランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示される ACE が 10 件未満となります。
Average(eps)	各間隔における平均レート（イベント数/秒）を表示します。 セキュリティ アプライアンスは、合計 30 回の完了したバースト間隔で、各バースト期間の終了時にカウント数を保存します。現在進行中の未完了バースト間隔は、平均レートに含まれません。たとえば、平均レート間隔が 20 分の場合、バースト間隔は 20 秒になります。最後のバースト間隔が 3:00:00 ～ 3:00:20 で、3:00:25 に **show** コマンドを使用すると、最後の 5 秒間は出力に含まれません。 このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔（1/30 個目）のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
Current(eps)	終了した最後のバースト間隔における現在バースト レート（イベント数/秒）を表示します。バースト間隔は、平均レート間隔の 1/30 と 10 秒のうち、どちらか大きいほうです。Average(eps) の説明の例では、現在のレートは 3:19:30 から 3:20:00 となります。
Trigger	アクセス リスト トラフィックがトリガーするレート制限は設定されていないため、この列は常に 0 です。この表示では許可されたトラフィックと拒否されたトラフィックが区別されません。**threat-detection basic-threat** コマンドを使用して基本脅威検出をイネーブルにすると、**show threat-detection rate access-list** コマンドを使用してアクセス リストの拒否を追跡できます。

表 13-5　　show threat-detection statistics top access-list のフィールド(続き)

フィールド	説明
Total events	各レート間隔におけるイベントの合計数を表示します。現在進行中の未完了バースト間隔は、合計イベント数に含まれません。このルールにおける唯一の例外は、合計イベント数を計算するときに、未完了バースト間隔のイベント数が最も古いバースト間隔(1/30 個目)のイベント数よりすでに多くなっている場合です。この場合、ASAは、最後の 29 回の完了間隔で合計イベント数を計算し、その時点での未完了バースト間隔のイベント数を加算します。この例外により、イベント数の大幅な増加をリアルタイムでモニタできます。
1-hour、8-hour	これらの固定レート間隔における統計情報を表示します。
acl_name/line_number	拒否される原因となった ACE のアクセス リスト名および行番号を表示します。

次に、**show threat-detection statistics top access-list rate-1** コマンドの出力例を示します。

```
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
```

次に、**show threat-detection statistics top port-protocol** コマンドの出力例を示します。

```
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
```

表 13-6 に、各フィールドの説明を示します。

表 13-6　show threat-detection statistics top port-protocol のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるポートまたはプロトコルのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるポート/プロトコルが 10 件未満となります。
Name	ポートまたはプロトコル名を表示します。
Id	ポート ID 番号またはプロトコル ID 番号を表示します。アスタリスク (*) は、その ID が IP プロトコル番号であることを意味します。
Average(eps)	表 13-2の説明を参照してください。
Current(eps)	表 13-2の説明を参照してください。
Trigger	ドロップされたパケット レートの制限値を超過した回数が表示されます。送受信バイトとパケットの行で指定された有効なトラフィックの場合、この値は常に 0 です。これは、有効なトラフィックをトリガーするレート制限がないためです。
Total events	表 13-2の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたポートおよびプロトコルから正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたポートおよびプロトコルから正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたポートおよびプロトコルから送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたポートおよびプロトコルで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
port_number/ *port_name*	パケットまたはバイトが送信、受信、またはドロップされた、ポートの番号と名前を表示します。
protocol_number/ *protocol_name*	パケットまたはバイトが送信、受信、またはドロップされた、プロトコルの番号と名前を表示します。

次に、**show threat-detection statistics top host** コマンドの出力例を示します。

```
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
```

表 13-7 に、各フィールドの説明を示します。

表 13-7　show threat-detection statistics top host のフィールド

フィールド	説明
Top	[0]（最高数）から [9]（最低数）の範囲で、統計情報の時間内かタイプにあるホストのランキングを表示します。統計情報が少なく、10 個のランクすべてが埋まらない場合は、表示されるホストが 10 件未満となります。
Average(eps)	表 13-2の説明を参照してください。
Current(eps)	表 13-2の説明を参照してください。
Trigger	表 13-2の説明を参照してください。
Total events	表 13-2の説明を参照してください。
Time_interval Sent byte	各期間において、表示されたホストに正常に送信されたバイト数を表示します。
Time_interval Sent packet	各期間において、表示されたホストに正常に送信されたパケット数を表示します。
Time_interval Sent drop	各期間において、スキャン攻撃の一部であったためにドロップされた、表示されたホストに送信されたパケット数を表示します。
Time_interval Recv byte	各期間において、表示されたホストで正常に受信したバイト数を表示します。
Time_interval Recv packet	一覧にあるポートおよびプロトコルが正常に受信したパケット数を、時間間隔ごとに表示します。
Time_interval Recv drop	一覧にあるポートおよびプロトコルが受信し、スキャン攻撃の一部であるためにドロップされたパケット数を、時間間隔ごとに表示します。
host_ip_address	パケットまたはバイトが送信、受信、ドロップされたホスト IP アドレスを表示します。

次に、**show threat-detection statistics top tcp-intercept** コマンドの出力例を示します。

```
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)
```

表 13-8 に、各フィールドの説明を示します。

表 13-8　　show threat-detection statistics top tcp-intercept のフィールド

フィールド	説明
Monitoring window size:	統計情報のためにASAがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval**コマンドを使用します。ASAは、この間隔でデータを 30 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常にレート間隔を 30 で割った数値になります。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	サンプリング期間中の平均攻撃レートを 1 秒あたりの攻撃数で表示します。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip	攻撃者の IP アドレスを表示します。
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。

次に、**show threat-detection statistics top tcp-intercept long** コマンドの出力例を示します。実際の送信元 IP アドレスがカッコ内に表示されています。

```
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)
```

次に、**show threat-detection statistics top tcp-intercept detail** コマンドの出力例を示します。

```
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
......
```

表 13-9 に、各フィールドの説明を示します。

表 13-9　show threat-detection statistics top tcp-intercept detail のフィールド

フィールド	説明
Monitoring window size:	統計情報のためにASAがデータをサンプリングする期間を表示します。デフォルトは 30 分です。この設定を変更するには、**threat-detection statistics tcp-intercept rate-interval**コマンドを使用します。ASAは、この間隔でデータを 30 回サンプリングします。
Sampling interval:	サンプリング間の間隔を表示します。この値は、常にレート間隔を 30 で割った数値になります。
rank	1 ～ 10 位のランキングを表示します。1 位は最も攻撃を受けたサーバで、10 位は最も攻撃が少なかったサーバです。
server_ip:port	攻撃を受けているサーバの IP アドレスおよびポートを表示します。
interface	サーバが攻撃を受けているインターフェイスを表示します。
avg_rate	**threat-detection statistics tcp-intercept rate-interval** コマンドで設定されたレート間隔での平均攻撃レートを、1 秒あたりの攻撃数で表示します（デフォルトのレート間隔は 30 分です）。レート間隔中、ASAは 30 秒ごとにデータをサンプリングします。
current_rate	現在の攻撃レート（1 秒あたりの攻撃数）を表示します。
total	攻撃の合計数を表示します。
attacker_ip or <*various*> Last: *attacker_ip*	攻撃者の IP アドレスを表示します。複数の攻撃者がいる場合は、「<various>」の後に最後の攻撃者の IP アドレスが表示されます。

表 13-9　show threat-detection statistics top tcp-intercept detail のフィールド(続き)

フィールド	説明
(*last_attack_time* ago)	最後の攻撃が発生した時間を表示します。
sampling data	30 個のサンプリング データ値をすべて表示します。間隔ごとの攻撃回数が表示されます。

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
threat-detection statistics	脅威の統計情報をイネーブルにします。

show tls-proxy

TLS プロキシおよびセッション情報を表示するには、グローバル コンフィギュレーション モードで **show tls-proxy** コマンドを使用します。

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

構文の説明

cert-dump	ローカル ダイナミック証明書をダンプします。出力は LDC の 16 進ダンプです。
count	セッション カウンタだけを表示します。
detail	各 SSL レッグおよび LDC の暗号を含む詳細な TLS プロキシ情報を表示します。
host *host_addr*	関連付けられたセッションを表示する特定のホストを指定します。
session	アクティブな TLS プロキシ セッションを表示します。
statistics	TLS セッションをモニタおよび管理するための統計情報を表示します。
tls_name	表示する TLS プロキシの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC モード	• Yes	• Yes	• Yes	• Yes	• Yes

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
8.3(1)	**statistics** キーワードが追加されました。

例

次に、**show tls-proxy** コマンドの出力例を示します。

```
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
```

次に、**show tls-proxy session** コマンドの出力例を示します。

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

次に、**show tls-proxy session detail** コマンドの出力例を示します。

```
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:
```

次に、**show tls-proxy session statistics** コマンドの出力例を示します。

```
ciscoasa# show tls-proxy session stastics
    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
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキー ペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
show running-config tls-proxy	すべてまたは指定された TLS プロキシの実行コンフィギュレーションを表示します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

show track

トラッキング プロセスが追跡したオブジェクトに関する情報を表示するには、ユーザ EXEC モードで **show track** コマンドを使用します。

show track [*track-id*]

構文の説明

track-id	トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

デフォルト

track-id が指定されなかった場合は、すべてのトラッキング オブジェクトに関する情報が表示されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ EXEC	• Yes	—	• Yes	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、**show track** コマンドの出力例を示します。

```
ciscoasa(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 3:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

関連コマンド

コマンド	説明
show running-config track	実行コンフィギュレーションの **track rtr** コマンドを表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

show traffic

インターフェイスの送信アクティビティと受信アクティビティを表示するには、特権 EXEC モードで **show traffic** コマンドを使用します。

show traffic

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• Yes	• Yes	• Yes	• Yes	• Yes

コマンド履歴

リリース	変更内容
7.2(1)	ASA 5550 の出力が追加されました。
9.3(1)	物理インターフェイスの集約トラフィックの出力が追加されました。
9.5(2)	SCTP および SCTP インスペクションが詳細な出力に追加されました。

使用上のガイドライン

show traffic コマンドは、**show traffic** コマンドが最後に入力された時点またはASA がオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、ASAが直前のリブート以降、オンラインになってからの経過時間です(直前のリブート以降に **clear traffic** コマンドが入力されていない場合)。コマンドが入力されていた場合は、コマンドが入力された時点からの経過時間となります。

ASA 5550 の場合、**show traffic** コマンドを実行するとスロットごとの集約スループットも表示されます。ASA 5550 のスループットを最大にするには、トラフィックをスロットに均一に分散する必要があります。この出力は、トラフィックが均一に分散しているかどうかを確認するのに役立ちます。

物理インターフェイスの集約トラフィックを表示するには、最初に **sysopt traffic detailed-statistics** コマンドを入力して、この機能をオンにする必要があります。

例

次に、**show traffic** コマンドの出力例を示します。

```
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/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
```

ASA 5550 の場合、次のテキストが最後に表示されます。

```
--------------------------------------
        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%|****************
```

次に、物理インターフェイスの集約トラフィック用に追加された出力例を示します。

```
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
```

関連コマンド

コマンド	説明
clear traffic	送信アクティビティと受信アクティビティのカウンタをリセットします。