



show t

- [show tcpstat](#) (2 ページ)
- [show tech-support](#) (5 ページ)
- [show telemetry](#) (9 ページ)
- [show terminal](#) (11 ページ)
- [show threat-detection memory](#) (13 ページ)
- [show threat-detection rate](#) (15 ページ)
- [show threat-detection scanning-threat](#) (18 ページ)
- [show threat-detection shun](#) (20 ページ)
- [show threat-detection statistics host](#) (22 ページ)
- [show threat-detection statistics port](#) (27 ページ)
- [show threat-detection statistics protocol](#) (31 ページ)
- [show threat-detection statistics top](#) (35 ページ)
- [show time-range](#) (45 ページ)
- [show tls-proxy](#) (46 ページ)
- [show track](#) (49 ページ)
- [show traffic](#) (50 ページ)

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。

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。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリー 変更内容
ス

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 1: **show tcpstat** コマンドの TCP 統計情報

統計	説明
tcb_cnt	TCP ユーザーの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザー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_rev good pkts	TCP スタックが受信した正常なパケットの数。
tcp_rev drop pkts	TCP スタックがドロップした受信パケットの数。
tcp_bad checksum	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 ユーザーの数。

統計	説明
tcp user hash add dup	新しい TCP ユーザーをハッシュ テーブルに追加しようとしたとき、そのユーザーがすでにテーブル内に存在していた回数。
tcp user srch hash hit	検索時にハッシュ テーブル内で TCP ユーザーが検出された回数。
tcp user srch hash miss	検索時にハッシュ テーブル内で TCP ユーザーが検出されなかった回数。
tcp user hash delete	TCP ユーザーがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザーを削除しようとしたとき、そのユーザーがハッシュ テーブル内で検出されなかった回数。
lip	TCP ユーザーのローカル IP アドレス。
fip	TCP ユーザーの外部 IP アドレス。
lp	TCP ユーザーのローカル ポート。
fp	TCP ユーザーの外部ポート。
st	TCP ユーザーの状態 (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 ユーザーの再送信キューの長さ。
inqlen	TCP ユーザーの入力キューの長さ。
tw_timer	TCP ユーザーの time_wait タイマーの値 (ミリ秒)。
to_timer	TCP ユーザー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 ユーザーのクローズ要求タイマーの値 (ミリ秒)。
per_timer	TCP ユーザーの持続タイマーの値 (ミリ秒)。
rt_timer	TCP ユーザーの再送信タイマーの値 (ミリ秒)。

統計	説明
tries	TCP ユーザーの再送信回数。

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** | **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。

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。

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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	detail 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。

リリース	変更内容
9.2(1)	出力が拡張され、 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 コマンドの情報が含まれるようになりました。 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。
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 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)	<p>show tech-support コマンドが次のようになりました。</p> <ul style="list-style-type: none"> • 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：このコマンドの出力は show tech-support detail の出力内に残されます。

リリース	変更内容
9.7(1)	<p>show tech-support コマンドは更新され、次の変更が加えられました。</p> <ul style="list-style-type: none"> 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。これで、ASA 仮想が現在稼働しているハイパーバイザが判別されます。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。
9.12(1)	<p>show ipv6 interface、show aaa-server、および show fragment の出力が show tech-support の出力に追加されました。</p>
9.13(1)	<p>show flow-offload info detail、show flow-offload statistics、および show asp table socket コマンドが追加されました。</p>
9.14(1)	<p>、show ssl objects and show ssl errors was added to the output of show tech-support.</p> <p>9.12(4) でも同様</p>
9.16(1)	<p>show tech-support コマンドが拡張され、次の変更が加えられました。</p> <ul style="list-style-type: none"> 最後の起動時の DPDK ログメッセージを含む showcontroller コマンドの出力。 仮想マシン (VM) の空きメモリと使用済みメモリ、共有メモリ、およびバッファに関する meminfo 統計情報。 ブート中に渡されるオプションと引数に関する cmdline 統計情報。
9.17(1)	<p>show access-list element-count および show asp rule-engine からの出力が追加されました。</p> <p>show tech-support コマンドの出力に、現在の DPDK メモリプールの統計情報が含まれるようになりました。</p>

リリース	変更内容
9.20(2)	このコマンドの出力には、 statistics all 、 statistics events 、 statistics np-clients 、 statistics cp-clients 、および statistics bulk-sync 統計情報の出力が含まれません。

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るさまざまな情報を入手します。

例

次に、**show tech-support** の出力を disk0 上のファイルに保存する例を示します。この出力は非常に長いので、結果を画面に送ると表示されるまでに時間がかかります。

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



- (注) show コマンドの実行中に **terminal pager 0** コマンドを使用しないでください。CPU の負荷が大きくなる可能性があります。CPU の過負荷により、ASA の通信障害が発生する可能性があるため、デフォルトの構成端末ページャ設定 (25 行) を使用します。

関連コマンド

コマンド	説明
show clock	Syslog サーバー (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 telemetry

テレメトリデータを表示するには、特権 EXEC モードで **show telemetry** コマンドを、いずれかのキーワードを指定して使用します。データが JSON 形式で表示されます。

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

構文の説明

history (オプション) テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示します。

last-report (オプション) FXOS に送信された最新のテレメトリデータを JSON 形式で表示します。

sample (オプション) 即時に生成されたテレメトリデータを JSON 形式で表示します。

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。

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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース 変更内容
ス

9.13(1) コマンドが追加されました。

使用上のガイドライン

service telemetry コマンドはデフォルトで有効になっています。最後に送信したテレメトリデータを表示するか、テレメトリの設定とアクティビティに関連する最新の 100 イベントを表示するかを選択できます。

例

次に、**show telemetry history** コマンドの出力例を示します。

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

関連コマンド

コマンド	説明
no service telemetry	テレメトリサービスを無効にします。
show running-config	設定されているデフォルト以外のテレメトリ設定のみを表示します。
show running-config all	設定済みのテレメトリ設定を表示します。

show terminal

現在の CLI セッションの端末設定を表示するには、特権 EXEC モードで **show terminal** コマンドを使用します。

show terminal

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。

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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース 変更内容
ス

7.0(1) コマンドが追加されました。

使用上のガイドライン

次のコマンドを使用して端末のプロパティを設定します。

- **terminal interactive** : CLI で ? を入力すると、現在の CLI セッションでヘルプを有効にします。
- **terminal monitor** : 現在の CLI セッションで syslog メッセージが表示されるようにします。
- **terminal width** : コンソールセッション中に表示する情報の幅を設定します。

show terminal コマンドでは **terminal pager** の設定は表示されません。

例

次に、**show terminal** コマンドの出力例を示します。

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

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。

コマンド	説明
pager	Telnetセッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal interactive	CLIで?を入力すると、現在のCLIセッションでヘルプを有効にします。
terminal monitor	現在のCLIセッションでsyslogメッセージが表示されるようにします。
terminal pager	Telnetセッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	コンソールセッション中に表示する情報の幅を設定します。

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。

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	• 対応	• 対応	• 対応	—	—

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ーできます。

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 <i>min_display_rate</i>	(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。 <i>min_display_rate</i> 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。ファイアウォール関連以外のドロップ (interface-drop 、 inspect-drop 、 scanning-threat) 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спек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ーします。フルスキャン脅威検出 (threat-detection scanning-threat コマンドを参照) では、このスキャン攻撃レート情報を収集し、ホストを攻撃者として分類して自動的に遮断することによって対処します。
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。

コマンド 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	• 対応	• 対応	• 対応	—	—

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、シビラティ (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

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、最後の 59 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ーできます。

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。

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。

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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

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、シビラティ（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。

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。

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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース 変更内容
ス

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、シビラティ（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。

コマンド	説明
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

<i>ip_address</i>	(任意) 特定のホストの統計情報を表示します。
<i>mask</i>	(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 <i>min_display_rate</i>	(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。 <i>min_display_rate</i> は、0 ~ 2147483647 の値に設定できます。

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。

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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース 変更内容
ス

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、シビラティ (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ーできます。

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

フィールド	説明
ホスト (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 packets 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 秒以内にサーバー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 <code>HOST_PORT_CLOSE</code> 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ーできます。

フィールド	説明
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ーできます。
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。

コマンド	説明
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 [<i>-end_port</i>]	(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 <i>min_display_rate</i>	(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。 <i>min_display_rate</i> は、0～2147483647 の値に設定できます。

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。

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	• 対応	• 対応	• 対応	—	—

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、シビラティ (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ーできます。

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

フィールド	説明
Average(eps)	<p>各間隔における平均レート（イベント数/秒）を表示します。</p> <p>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。</p> <p>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ーできます。</p>
Current(eps)	<p>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。</p>
Trigger	<p>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。</p>
Total events	<p>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ーできます。</p>
port_number /port_name	<p>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。</p>
tot-ses	<p>このポートのセッションの合計数を表示します。</p>
act-ses	<p>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。</p>

フィールド	説明
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

<i>protocol_number</i>	(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 <i>min_display_rate</i>	(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。 <i>min_display_rate</i> は、0 ~ 2147483647 の値に設定できます。
<i>protocol_name</i>	(任意) 特定のプロトコル名の統計情報を表示します。 <ul style="list-style-type: none"> • ah • eigrp • esp • gre • icmp • igmp • igrp • ip • ipinip • ipsec • nos • ospf • pcp • pim • pptp • snp • tcp • udp

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。

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	• 対応	• 対応	• 対応	—	—

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、シビラティ（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、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ーできます。

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 13-2 に、各フィールドの説明を示します。

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

フィールド	説明
Average(eps)	<p>各間隔における平均レート（イベント数/秒）を表示します。</p> <p>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。</p> <p>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ーできます。</p>
Current(eps)	<p>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。</p>
Trigger	<p>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。</p>
Total events	<p>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ーできます。</p>
<i>protocol_number</i> <i>/protocol_name</i>	<p>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。</p>

フィールド	説明
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、IP プロトコル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ー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) サーバーの実際の 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 <i>min_display_rate</i>	(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。 <i>min_display_rate</i> 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 サーバーが含まれます。

コマンド 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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

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、シビラティ (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ーできます。

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 13-2 に、各フィールドの説明を示します。

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

フィールド	説明
上	[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。

フィールド	説明
Average(eps)	<p>各間隔における平均レート（イベント数/秒）を表示します。</p> <p>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。</p> <p>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ーできます。</p>
Current(eps)	<p>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。</p>
Trigger	<p>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。</p>
Total events	<p>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ーできます。</p>
1-hour、8-hour	<p>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。</p>
<i>acl_name</i> <i>/line_number</i>	<p>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。</p>

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

フィールド	説明
上	[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。
名前	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。

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	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。

例

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

フィールド	説明
上	[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。
トリガー	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。

フィールド	説明
<i>Time_interval</i> 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。
<i>host_ip_address</i>	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。

例

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)
```

に、各フィールドの説明を示します。

表 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。
<i>rank</i>	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ーで、10 位は最も攻撃が少なかったサーバーです。
<i>server_ip:port</i>	攻撃を受けているサーバーの IP アドレスおよびポートを表示します。
<i>interface</i>	サーバーが攻撃を受けているインターフェイスを表示します。
<i>avg_rate</i>	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。

フィールド	説明
<i>current_rate</i>	現在の攻撃レート（1秒あたりの攻撃数）を表示します。
<i>total</i>	攻撃の合計数を表示します。
<i>attacker_ip</i>	攻撃者のIPアドレスを表示します。
<i>(last_attack_time ago)</i>	最後の攻撃が発生した時間を表示します。

例

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 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ーで、10位は最も攻撃が少なかったサーバーです。
server_ip:port	攻撃を受けているサーバーの IP アドレスおよびポートを表示します。
interface	サーバー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。
(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 time-range

すべての時間範囲オブジェクトの設定を表示するには、特権 EXEC モードで **show time-range** コマンドを使用します。

show time-range [*name*]

構文の説明

name (オプション) この時間範囲オブジェクトの情報のみを表示します。

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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース 変更内容
ス

7.0(1) このコマンドが追加されました。

例

次に、時間範囲オブジェクトの設定を表示する例を示します。この例では、work-hours という名前のオブジェクトが1つあります。inactive は、オブジェクトが使用されていないことを意味します。

```
ciscoasa# show time-range

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

関連コマンド

コマンド	説明
time-range	時間範囲オブジェクトを設定します。

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 [cert-dump]	各SSLログおよびLDCの暗号を含む詳細なTLSプロキシ情報を表示します。 cert-dump キーワードを追加して、ローカルダイナミック証明書(LDC)の16進ダンプを取得します。 また、これらのキーワードは、 host オプションとともに使用できます。
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のIPv4またはIPv6アドレスを指定します。
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ー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。

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。

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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース 変更内容
ス

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: 0
Per-Session Licensed TLS Proxy Sessions
(Established: 222, License Limit: 3000)
  SIP: 2
  SCCP: 20
  DIAMETER: 200
Total TLS Proxy Sessions
  Established: 822
  Platform Limit: 1000
```

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

セキュリティレベル合意（SLA）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、ユーザー 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 オブジェクト ID 番号（1～500）。

コマンド 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。

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
ユーザー EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリー 変更内容
ス

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 03:41:16
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。

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。

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	• 対応	• 対応	• 対応	• 対応	• 対応

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 が直前のレポート以降、オンラインになってからの経過時間です（直前のレポート以降に **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/secEthernet0:
              received (in 102.080 secs):      2049 packets 233027 bytes
              20 pkts/sec 2282 bytes/sec      transmitted (in 102.080 secs):      2048
              packets 232750 bytes      20 pkts/sec 2280 bytes/sec

```

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

```

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。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。