従来型デバイスのコマンド ライン リファレンス

このリファレンスでは、次のデバイスのコマンドライン インターフェイス（CLI）について説明します。

- 7000 および 8000 シリーズ
- ASA FirePOWER
- NGIPSv

（注） Firepower Management Center で CLI を使用することはできません。Firepower Management Center は、Linux シェル アクセスをサポートし、Cisco Technical Assistance Center（TAC） の監督下でのみサポートされます。

（注） Firepower Threat Defense コマンド リファレンスについては、『Command Reference for Firepower Threat Defense』を参照してください。

CLI について

デバイスに CLI（従来型デバイスでのコマンドライン インターフェイスへのログイン または Firepower Threat Defense デバイスのコマンドライン インターフェイスへのログイン を参照）を

使用してログインすると、この章で説明するコマンドを使用して、デバイスを表示、設定、およびトラブルシューティングすることができます。

（注） 7000 または 8000 シリーズ デバイスをリブートし、できるだけ早く CLI にログインしても、Web インターフェイスが使用できるようになるまで、実行するすべてのコマンドは監査ログに記録されません。

CLI コマンドでは大文字と小文字が区別されません。ただし、ユーザ名や検索フィルタなど、テキストが CLI フレームワークの一部ではないパラメータでは区別されるので注意してください。

関連トピック

Firepower システムのユーザ インターフェイス

CLI モード

CLI モードには `show` や `configure` など多数あり、これらのモードにはモード名で始まる一連のコマンドが含まれています。モードを開始して、そのモードで有効なコマンドを入力することも、任意のモードからフル コマンドを入力することもできます。たとえば、Analyst1 というユーザ アカウントの情報を表示するには、CLI プロンプトで次のように入力します。

```
show user Analyst1
```

すでに `show` モードを開始している場合は、CLI プロンプトで次のように入力します。

```
user Analyst1
```

CLI アクセス レベル

各モードで、ユーザが使用できるコマンドは、ユーザの CLI アクセスによって異なります。ユーザ アカウントを作成する場合は、手動で次のいずれかの CLI アクセス レベルに割り当てることができます。

- [基本（Basic）]：ユーザは読み取り専用のアクセス権を持ち、システム パフォーマンスに影響を与えるコマンドを実行することはできません。
- [設定（Configuration）]：ユーザは、読み取り/書き込みアクセス権があり、システム パフォーマンスに影響を与えるコマンドを実行することができます。
- [なし（None）]：ユーザはシェルにログインできません。

7000 および 8000 シリーズ デバイスでは、Web インターフェイスの [ユーザ管理（User Management）] ページでコマンド ラインの権限を割り当てることができます。NGIPSv と ASA FirePOWER では、CLI を使用してコマンド ラインの権限を割り当てます。

基本的な CLI コマンド

基本的なCLIコマンドを使用して、CLIとやりとりすることができます。これらのコマンドはデバイスの動作に影響しません。基本的なコマンドは、すべてのCLIユーザが使用可能です。

configure password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLIは現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを2回入力するよう要求します。

アクセス（Access）

基本

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

終了

ユーザをデフォルトのモードに戻します。（ユーザは、いずれかの下位レベルのCLIコンテキストから上位のデフォルト モードへ移動します）。

アクセス（Access）

基本

構文

```
end
```

例

```
configure network ipv4> end
>
```

exit

CLI コンテキストを、次に高い CLI コンテキスト レベルへ移動します。デフォルト モードからこのコマンドを発行すると、ユーザは現行の CLI セッションからログアウトします。これは、CLI コマンドの `logout` を発行するのと同じです。

アクセス（Access）

基本

構文

```
exit
```

例

```
configure network ipv4> exit
configure network>
```

ヘルプ

CLI 構文の概要を表示します。

アクセス（Access）

基本

構文

```
help
```

例

```
> help
```

history

現行のセッションのコマンドラインの履歴を表示します。

アクセス（Access）

基本

構文

```
history limit
```

ここで `limit` は履歴リストのサイズを設定します。サイズを無制限に設定するには、0 を入力します。

例

```
history 25
```

ログアウト

現行の CLI コンソール セッションから現行のユーザをログアウトします。

アクセス（Access）

基本

構文

```
logout
```

例

```
> logout
```

?（疑問符）

CLI コマンドと CLI パラメータの状況依存ヘルプを表示します。以下のように疑問符（?）コマンドを使用します。

- 現在の CLI コンテキストで使用できるコマンドのヘルプを表示するには、コマンド プロンプトに疑問符（?）を入力します。
- 特定の文字列セットで始まる使用可能なコマンドのリストを表示するには、疑問符（?）の直後に短縮コマンドを入力します。
- コマンドの法的引数のヘルプを表示するには、コマンドプロンプトの引数の代わりに疑問符（?）を入力します。

疑問符（?）は、コンソールにエコーバックすることはない点にご注意ください。

アクセス（Access）

基本

構文

```
?
abbreviated_command ?
command [arguments] ?
```

例

```
> ?
```

?? （二重の疑問符）

CLI コマンドおよびパラメータの詳細な状況依存ヘルプを表示します。

アクセス（Access）

基本

構文

```
??
abbreviated_command end??
command [arguments] ??
```

例

```
> configure manager add ??
```

show コマンド

show コマンドは、デバイスの状態に関する情報を提供します。これらのコマンドはデバイスの動作モードを変更しません。また、これらのコマンドを実行しても、システムの動作に対する影響は最小限になります。ほとんどの show コマンドはすべての CLI ユーザが利用できますが、`show user` コマンドを発行できるのは、Configuration CLI アクセス権限を持つユーザのみです。

access-control-config

現在展開されている次のようなアクセス制御設定を表示します。

- セキュリティ インテリジェンスの設定
- アクセス コントロール ポリシーで呼び出されるあらゆるサブポリシーの名前
- 侵入変数セット データ

- ロギングの設定
- ポリシー レベルのパフォーマンス、前処理、全般設定などのその他の詳細設定

また、送信元と宛先ポートのデータ（ICMP エントリのタイプとコードを含む）および各アクセス コントロール ルールに一致する接続数（ヒット数）などの、ポリシーに関連する接続情報も表示します。

アクセス（Access）

基本

構文

```
show access-control-config
```

例

```
> show access-control-config
```

alarms

デバイスで現在アクティブ（障害/停止）状態になっているハードウェアのアラームを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show alarms
```

例

```
> show alarms
```

arp-tables

ネットワークに適用できる Address Resolution Protocol テーブルを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show arp-tables
```

例

```
> show arp-tables
```

audit-log

監査ログを時系列の逆順に表示します。最も新しい監査ログ イベントが先頭になります。

アクセス（Access）

基本

構文

```
show audit-log
```

例

```
> show audit-log
```

audit_cert

現行の監査ログ クライアント証明書を表示します。

アクセス（Access）

基本

構文

```
show audit_cert
```

例

```
> show audit_cert
```

bypass

7000 または 8000 シリーズ デバイスで、使用中のインライン セットを一覧表示し、それらのセットについて次のいずれかのバイパス モード ステータスを表示します。

- `armed`：インターフェイス ペアが、障害発生時にハードウェア バイパスになるように設定されている（[バイパス モード：バイパス（Bypass Mode: Bypass）]）か、または、**configure bypass close** コマンドを使用して強制的にフェールクローズされました。
- `engaged`：インターフェイス ペアが、オープンに失敗したか、または、**configure bypass open** コマンドを使用して強制的にハードウェア バイパスになりました。
- `off`：インターフェイス ペアがフェールクローズ（[バイパス モード：非バイパス（Bypass Mode: Non-Bypass）]）に設定されており、インターフェイス ペアで障害が発生した場合にはパケットがブロックされます。

アクセス（Access）

基本

構文

```
show bypass
```

例

```
> show bypass
s1p1 ↔ s1p2: status 'armed'
s1p1 ↔ s1p2: status 'engaged'
```

High-availability コマンド

ハイ アベイラビリティの設定、ステータス、メンバー デバイスまたはスタックの情報を表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

config

デバイスの高可用性の設定を表示します。

構文

```
show high-availability config
```

例

```
> show high-availability config
```

high-availability ha-statistics

高可用性ペアのデバイスの状態共有統計を表示します。

構文

```
show high-availability ha-statistics
```

例

```
> show high-availability ha-statistics
```

cpu

デバイス上のすべての CPU のプラットフォームに適合する現行の CPU の使用率の統計情報を表示します。7000 および 8000 シリーズ デバイスでは、次の値が表示されます。

- CPU：プロセッサ番号。
- ロード：0 ～ 100 の数値で表される CPU 使用率。0 はロードされていない状態で、100 は完全にロードされたことを表します。

NGIPSv および ASA FirePOWER では、次の値が表示されます。

- CPU：プロセッサ番号。
- %user：ユーザ レベル（アプリケーション）で実行中に生じたCPU使用率の割合（パーセンテージ）。
- %nice：高い優先度のユーザ レベルで実行中に生じた CPU 使用率の割合（パーセンテージ）。
- %sys：システム レベル（カーネル）で実行中に生じた CPU 使用率の割合（パーセンテージ）。これには、サービスの割り込みや softirqs で経過する時間は含まれません。softirq（ソフトウェアの割り込み）は、複数の CPU で同時に実行できる最大 32 個の列挙されたソフトウェア割り込みの 1 つです。
- %iowait：システムに未処理のディスク I/O 要求があったときに、CPU がアイドル状態だった時間の割合（パーセンテージ）。
- %irq：割り込みを行うために CPU が費やした時間の割合（パーセンテージ）。
- %soft：softirqs を行うために CPU が費やした時間の割合（パーセンテージ）。

- %steal：ハイパーバイザが別の仮想プロセッサを実行しているときに、仮想CPUが強制的な待機で費やした時間の割合（パーセンテージ）。
- %guest：仮想プロセッサを実行するためにCPUが費やした時間の割合（パーセンテージ）。
- %idle：CPUがアイドル状態で、システムに未処理のディスクI/O要求がなかった時間の割合（パーセンテージ）。

アクセス（Access）

基本

構文

```
show cpu [procnum]
```

ここで`procnum`は、使用率の情報を表示するプロセッサの数を表します。有効な値は0から、システム上の合計プロセッサ数から1引いた数までの範囲です。`procnum`が7000または8000シリーズデバイスで使用されている場合は無視されます。このプラットフォームについては、使用率の情報はすべてのプロセッサについてのみ表示されるためです。

例

```
> show cpu
```

Database コマンド

データベースの表示（`show database`）コマンドは、デバイスの管理インターフェイスを設定します。

アクセス（Access）

基本

processes

実行中のデータベース クエリのリストを表示します。

アクセス（Access）

基本

構文

```
show database processes
```

例

```
> show database processes
```

slow-query-log

データベースのスロー クエリ ログを表示します。

アクセス（Access）

基本

構文

```
show database slow-query-log
```

例

```
> show database slow-query-log
```

device-settings

現行のデバイスに特有のアプリケーションのバイパス設定に関する情報を表示します。

アクセス（Access）

基本

構文

```
show device-settings
```

例

```
> show device-settings
```

disk

現行のディスクの使用率を表示します。

アクセス（Access）

基本

構文

```
show disk
```

例

```
> show disk
```

disk-manager

システムの各パート（サイロ、低水位、高水位など）のディスク使用率の詳細情報を表示します。

アクセス（Access）

基本

構文

```
show disk-manager
```

例

```
> show disk-manager
```

dns

現行の DNS サーバのアドレスと検索ドメインを表示します。

アクセス（Access）

基本

構文

```
show dns
```

例

```
> show dns
```

expert

シェルを起動します。

アクセス（Access）

基本

構文

```
expert
```

例

```
> expert
```

fan-status

ハードウェア ファンの現在のステータスを表示します。このコマンドは NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show fan-status
```

例

```
> show fan-status
```

fastpath-rules

現在設定されている 8000 シリーズ の fastpath ルールを表示します。このコマンドは 8000 シリーズ デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show fastpath-rules
```

例

```
> show fastpath-rules
```

gui

Web インターフェイスの現在の状態を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show gui
```

例

```
> show gui
```

hostname

デバイスのホスト名およびアプライアンス UUID を表示します。CLI を使用してデバイスのホスト名を編集する場合は、管理する Firepower Management Center に変更が反映されることを確認します。場合によっては、デバイス管理設定を手動で編集する必要があります。

アクセス（Access）

基本

構文

```
show hostname
```

例

```
> show hostname
```

hosts

ASA FirePOWER モジュールの /etc/hosts ファイルの内容を表示します。

アクセス（Access）

基本

構文

```
show hosts
```

例

```
> show hosts
```

hyperthreading

ハイパースレッディングが有効か無効かを表示します。このコマンドは ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show hyperthreading
```

例

```
> show hyperthreading
```

inline-sets

すべてのインライン セキュリティ ゾーンと関連するインターフェイスの設定データを表示します。このコマンドは ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show inline-sets
```

例

```
> show inline-sets
```

interfaces

パラメータが指定されていない場合は、設定されているすべてのインターフェイスのリストが表示されます。パラメータが指定されている場合は、指定されたインターフェイスの詳細情報が表示されます。

アクセス（Access）

基本

構文

```
show interfaces interface
```

ここで *interface* は詳細情報を表示する特定のインターフェイスです。

例

```
> show interfaces
```

ifconfig

ASA FirePOWER モジュールに対するインターフェイスの設定を表示します。

アクセス（Access）

基本

構文

```
show ifconfig
```

例

```
> show ifconfig
```

lcd

LCD のハードウェア ディスプレイが有効か無効かを表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show lcd
```

例

```
> show lcd
```

Link-aggregation コマンド

`show link-aggregation` コマンドは、リンク集約グループ（LAG）の設定および統計情報を表示します。このコマンドは、NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

設定：

LAG ID、インターフェイスの数、設定モード、ロード バランシング モード、LACP 情報、物理インターフェイスのタイプなど、設定された各 LAG の構成の詳細を表示します。

アクセス（Access）

基本

構文

```
show link-aggregation configuration
```

例

```
> show link-aggregation configuration
```

統計情報

ステータス、リンク ステートと速度、コンフィギュレーション モード、送受信されたパケットのカウンタ、および送受信されたバイトのカウンタなど、設定された各 LAG の統計情報をインターフェイスごとに表示します。

アクセス（Access）

基本

構文

```
show link-aggregation statistics
```

例

```
> show link-aggregation statistics
```

link-state

デバイスのポートのタイプ、リンク、スピード、速度、デュプレックスの状態およびバイパスモードを表示します。このコマンドは ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

構文

```
show link-state
```

例

```
> show link-state
```

log-ips-connection

記録された侵入イベントに関連付けられている接続イベントのロギングが有効か無効かを表示します。

アクセス（Access）

基本

構文

```
show log-ips-connection
```

例

```
> show log-ips-connection
```

managers

Firepower Management Center の設定および通信のステータスを表示します。登録キーおよび NAT ID は、登録が保留中の場合のみ表示されます。

デバイスが、スタック設定のセカンダリ デバイスとして設定されている場合、管理している両方の Management Center、およびプライマリ デバイスに関する情報が表示されます。

アクセス（Access）

基本

構文

```
show managers
```

例

```
> show managers
```

memory

デバイスの合計メモリ、使用中のメモリ、使用可能なメモリを表示します。

アクセス（Access）

基本

構文

```
show memory
```

例

```
> show memory
```

model

デバイスのモデル情報を表示します。

アクセス（Access）

基本

構文

```
show model
```

例

```
> show model
```

mpls-depth

管理インターフェイスに設定されている MPLS レイヤ数を 0～6 で表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show mpls-depth
```

例

```
> show mpls-depth
```

NAT コマンド

`show nat` コマンドは、管理インターフェイスの NAT データと設定情報を表示します。このコマンドは、NGIPSv および ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

active-dynamic

ダイナミック ルールに従って変換されている NAT フローを表示します。これらのエントリは、フローがルールに一致している場合に、ルールがタイムアウトになるまで表示されます。したがって、リストは正確ではないことがあります。タイムアウトはプロトコルに依存します。ICMP は 5 秒、UDP は 120 秒、TCP は 3600 秒、他のすべてのプロトコルは 60 秒です。

構文

```
show nat active-dynamic
```

例

```
> show nat active-dynamic
```

active-static

スタティック ルールに従って変換されている NAT フローを表示します。これらのエントリは、デバイスにルールが展開されるとすぐに表示されます。リストは、スタティックな NAT ルールに一致しているアクティブなフローを示しているわけではありません。

構文

```
show nat active-static
```

例

```
> show nat active-static
```

allocators

すべての NAT アロケータの情報、ダイナミック ルールで使用されている変換済みアドレスのプールを表示します。

構文

```
show nat allocators
```

例

```
> show nat allocators
```

config

管理インターフェイスの現在の NAT ポリシーの設定を表示します。

構文

```
show nat config
```

例

```
> show nat config
```

dynamic-rules

指定されたアロケータ ID を使用しているダイナミックな NAT ルールを表示します。

構文

```
show nat dynamic-rules allocator_id
```

ここで `allocator_id` は有効なアロケータ ID 番号です。

例

```
> show nat dynamic-rules 9
```

flows

指定されたアロケータ ID を使用しているルールについてフローの数を表示します。

構文

```
show nat flows allocator-id
```

ここで *allocator_id* は有効なアロケータ ID 番号です。

例

```
> show nat flows 81
```

static-rules

すべてのスタティック NAT ルールを表示します。

構文

```
show nat static-rules
```

例

```
> show nat static-rules
```

netstat

ASA FirePOWER モジュールのアクティブなネットワーク接続を表示します。

アクセス（Access）

基本

構文

```
show netstat
```

例

```
> show netstat
```

network

管理インターフェイスの IPv4 および IPv6 の設定、MAC アドレス、HTTP プロキシアドレス、ポート、ユーザ名（設定されている場合）を表示します。

アクセス（Access）

基本

構文

```
show network
```

例

```
> show network
```

network-modules

インストールされているすべてのモジュール、およびモジュールの情報（シリアル番号など）を表示します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show network-modules
```

例

```
> show network-modules
```

network-static-routes

インターフェイス、宛先アドレス、ネットワーク マスク、およびゲートウェイ アドレスなど、設定済みのすべてのネットワーク スタティック ルートとその情報が表示されます。

アクセス（Access）

基本

構文

```
show network-static-routes
```

例

```
> show network-static-routes
```

ntp

NTP コンフィギュレーションを表示します。

アクセス（Access）

基本

構文

```
show ntp
```

例

```
> show ntp
```

perfstats

デバイスのパフォーマンスの統計情報を表示します。

アクセス（Access）

基本

構文

```
show perfstats
```

例

```
> show perfstats
```

portstats

デバイスのすべての挿入されたポートのポート統計を表示します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

アクセス（Access）

基本

構文

```
show portstats [copper | fiber | internal | external | all]
```

銅線は、すべての銅線ポートを指定します。光ファイバはすべての光ファイバポートを指定します。内部はすべての内部ポートをします。外部はすべての外部（銅線および光ファイバ）ポートをします。すべてはすべてのポート（外部および内部）を指定します。

例

```
> show portstats fiber
```

power-supply-status

現在のハードウェアの電源状態を表示します。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

（注） 8000 シリーズ 管理対象デバイスで電源障害が発生すると、CLI コマンドの show power-supply-status が正しいステータスを反映するまでに 15 分かかる場合があります。

アクセス（Access）

基本

構文

```
show power-supply-status
```

例

```
> show power-supply-status
```

process-tree

デバイスで実行中のプロセスについて、タイプごとにツリー形式でソートして表示します。

アクセス（Access）

基本

構文

```
show process-tree
```

例

```
> show process-tree
```

processes

デバイス上で現在実行中のプロセスについて、CPU 使用率の降順で表示します。

アクセス（Access）

基本

構文

```
show processes sort-flag filter
```

ここで、メモリ（の降順）でソートする場合は、*sort-flag* に -m を指定し、プロセス名ではなくユーザ名でソートする場合は -u を指定します。また、コマンドのフルネームおよびパスを表示する場合は verbose を指定します。*filter* パラメータは、コマンドの検索語または結果をフィルタするために使用するユーザ名を指定します。見出し行は表示されたままです。

例

```
> show processes -u user1
```

ルート

ASA FirePOWER モジュールに関するルーティング情報を表示します。

アクセス（Access）

基本

構文

```
show route
```

例

```
> show route
```

routing-table

パラメータが指定されていない場合は、すべての仮想ルータに関するルーティング情報を表示します。パラメータが指定されている場合は、指定のルータに関するルーティング情報や、該当する場合には、指定のルーティング プロトコル タイプを表示します。パラメータはすべてオプションです。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show routing-table name [ ospf | rip | static ]
```

name は、情報を必要とする特定のルータ名です。ospf、rip、static は、ルーティング プロトコル タイプを指定します。

例

```
> show routing-table Vrouter1 static
```

serial-number

シャーシのシリアル番号を表示します。このコマンドは NGIPSv では使用できません。

アクセス（Access）

基本

構文

```
show serial-number
```

例

```
> show serial-number
```

ssl-policy-config

現在適用されている SSL ポリシーの設定（ポリシーの説明、デフォルトのロギング設定、有効なすべての SSL ルールとルールの設定など）、信頼できる CA 証明書、および復号化不可能なトラフィックのアクションを表示します。

アクセス（Access）

基本

構文

```
show ssl-policy-config
```

例

```
> show ssl-policy-config
```

stacking

管理対象デバイスのスタッキングの設定とポジションを表示します。プライマリとして設定されているデバイスでは、すべてのセカンダリ デバイスのデータも示されます。高可用性ペアの

スタックの場合、このコマンドは、スタックが高可用性ペアのメンバーであることも示します。スタッキングを有効または無効にする（大半の場合は無効にする）には、ユーザは Web インターフェイスを使用する必要があります。スタッキングが有効になっていない場合、コマンドは `Stacking not currently configured` というメッセージを返します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show stacking
```

例

```
> show stacking
```

summary

デバイスに関して最もよく使用される情報（バージョン、タイプ、UUID など）のサマリーを表示します。詳細は次の `show` コマンドを参照してください。`version`、`interfaces`、`device-settings`、および `access-control-config`。

アクセス（Access）

基本

構文

```
show summary
```

例

```
> show summary
```

syslog

システムのログを時系列の逆順で表示します。オプションでフィルタを指定して、ページビューごとに表示するコンテンツとレコード数に基づいて（デフォルトは25）、特定のレコードを表示できます。

アクセス（Access）

基本

構文

```
show syslog ["filter" records_per_page]
```

filter が Grep 互換の検索フィルタを指定し、*records_per_page* が各ページ ビューに表示するレコード数を指定する場合。検索フィルタの詳細については、「システム ログ フィルタの構文」を参照してください。

例

```
> show syslog "ssh" 20
```

システムは文字列「ssh」を含む 20 件の直近の syslog レコードを表示します。次の 20 件のレコードを表示するには Enter キーを押し、表示を停止するには q を入力します。

時刻

現在の日付と時刻を、UTC および現行のユーザに設定されているローカル タイム ゾーンで表示します。

アクセス（Access）

基本

構文

```
show time
```

例

```
> show time
```

traffic-statistics

パラメータが指定されていない場合は、すべてのポートから送信された、および受信したバイトの詳細情報を表示します。ポートが指定されている場合は、指定されたポートの情報のみを表示します。ASA FirePOWER モジュールに対してポートを指定することはできません。システムはデータ プレーン インターフェイスのみを表示します。

アクセス（Access）

基本

構文

```
show traffic-statistics port
```

ここで *port* は、情報を表示させたい特定のポートです。

例

```
> show traffic-statistics s1p1
```

user

NGIPSv のみに適用できます。指定されたユーザに関する設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（`Yes` または `No`）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（`N/A` または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス（**Access**）

設定（Configuration）

構文

```
show user username username username ...
```

ここで *username* はユーザの名前を表します。複数の username はスペースで区切って指定します。

例

```
> show user jdoe
```

ユーザ

NGIPSv のみに適用できます。すべてのローカル ユーザの設定の詳細情報を表示します。次の値が表示されます。

- Login：ログイン名
- UID：ユーザ ID（数値）
- Auth（`Local` または `Remote`）：ユーザがどのように認証されているか
- Access（`Basic` または `Config`）：ユーザの権限レベル
- Enabled（`Enabled` または `Disabled`）：ユーザがアクティブかどうか
- Reset（`Yes` または `No`）：次のログイン時にユーザがパスワードを変更する必要があるかどうか
- Exp（`Never` または数値）：ユーザのパスワード変更が必要になるまでの日数
- Warn（`N/A` または数値）：パスワードの有効期限が切れる前に、ユーザがパスワード変更のために与えられる日数
- Str（`Yes` または `No`）：ユーザのパスワードが強度チェックの基準を満たす必要があるかどうか
- Lock（`Yes` または `No`）：ログインの失敗が多すぎる場合に、ユーザのアカウントがロックされるかどうか
- Max（`N/A` または数値）：ユーザのアカウントがロックされる前に失敗するログインの最大回数

アクセス（**Access**）

設定（Configuration）

構文

```
show users
```

例

```
> show users
```

version

製品のバージョンとビルドを表示します。detail パラメータが指定されている場合は、追加のコンポーネントのバージョンが表示されます。

アクセス（Access）

基本

構文

```
show version [detail]
```

例

```
> show version
```

virtual-routers

パラメータが指定されていない場合は、現在設定されているすべての仮想ルータのリスト、および DHCP リレー、OSPF、および RIP の情報が表示されます。パラメータが指定されている場合は、指定されたルータに関する情報が、指定されたルート タイプによって制限されて表示されます。パラメータはすべてオプションです。このコマンドはNGIPSvおよびASA FirePOWERでは使用できません。

アクセス（Access）

基本

構文

```
show virtual-routers [ dhcprelay | ospf | rip ] name
```

ここで `dhcprelay`、`ospf`、および `rip` はルート タイプを表します。*name* は、情報を表示する特定のルータの名前を表します。`ospf` を指定した場合は、ルート タイプ、および（存在する場合は）ルート名に対して `neighbors`、`topology`、または `lsadb` を指定することができます。

例

```
> show virtual-routers ospf VRouter2
```

virtual-switches

パラメータが指定されていない場合は、設定されているすべての仮想スイッチのリストが表示されます。パラメータが指定されている場合は、指定されたスイッチに関する情報が表示されます。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

基本

構文

```
show virtual-switches name
```

例

```
> show virtual-switches Vswitch1
```

vmware-tools

VMware Tools が、仮想デバイス上で現在有効になっているかどうかを示します。このコマンドは、NGIPSv のみで使用できます。

VMware ツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティ スイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト（http://www.vmware.com）を参照してください。

アクセス（Access）

基本

構文

```
show vmware-tools
```

例

```
> show vmware-tools
```

VPN コマンド

`show VPN` コマンドは、VPN ステータス、および VPN 接続の設定情報を表示します。このコマンドは、NGIPSv デバイスと ASA FirePOWER デバイスでは使用できません。

アクセス（Access）

基本

config

すべての VPN 接続の設定を表示します。

構文

```
show vpn config
```

例

```
> show vpn config
```

config by virtual router

仮想ルータについて、すべての VPN 接続の設定を表示します。

構文

```
show vpn config virtual router
```

例

```
> show vpn config VRouter1
```

status

VPN 接続すべてのステータスを表示します。

構文

```
show vpn status
```

例

```
> show vpn status
```

status by virtual router

仮想ルータについて、すべての VPN 接続のステータスを表示します。

構文

```
show vpn status virtual router
```

例

```
> show vpn status VRouter1
```

counters

すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters
```

例

```
> show vpn counters
```

counters by virtual router

仮想ルータについて、すべての VPN 接続のカウンタを表示します。

構文

```
show vpn counters virtual router
```

例

```
> show vpn counters VRouter1
```

コンフィギュレーション コマンド

コンフィギュレーション コマンドを使用して、システムを設定および管理することができます。これらのコマンドはシステムの動作に影響を与えます。そのため、基本（Baisc）レベルのパスワード設定（configure password）コマンドを除き、設定 CLI アクセス権限を持つユーザのみがこれらのコマンドを発行できます。

audit_cert コマンド

audit_cert コマンドは、安全性監査ログ ストリーミングを行うためにデバイスの監査ログ クライアント証明書の設定を行います。

アクセス（Access）

設定（Configuration）

削除

セキュアな監査ログ ストリーミングの現行のクライアント証明書を削除します。

構文

```
configure audit_cert delete
```

例

```
> configure audit_cert delete
```

import

セキュアな監査ログストリーミングのクライアント証明書をインポートします。ユーザは、コマンドを入力すると、クライアント証明書と秘密キー、または証明書チェーンをCLIから入力するように求められます。

構文

```
configure audit_cert import
```

例

```
> configure audit_cert import
***************Import Audit Client Certificate**************

1 Import Client Certificate and Private Key
```

```
2 Import Certificate Chain
0 Exit

************************************************************
Enter choice: 1
Enter your audit client certificate (PEM format) here:
-----BEGIN CERTIFICATE-----
MIIEoTCCA4mgAwIBAgICAR4wDQYJK0ZIhvcNaQALBWAugYICzAJBqNVBATYAiVT
   ...certificate details ...
Tx*FAhnXeUZ78hFepg1yHQMYWTkD7hCqmSN3UkAb1l0IoBcxTA==
-----END CERTIFICATE-----

Enter your private key (PEM format) here:
-----BEGIN RSA PRIVATE KEY-----
miiieOWobabkc3qwaOgVx0Tt61eY83Mrqa+bek_qPetcHRAw6ea4p0TlMVVsE7qr
   ...private key details ...
nRI6QNkoumLUT9EvjF6bFoT3M6eDI7+NdDIhjVeOP*E4+hxEX50jM
-----END RSA PRIVATE KEY-----

Client certificate import succeed, exiting...
```

bypass

7000 または 8000 シリーズ デバイスで、インライン ペアをフェールオープン（ハードウェア バイパス）モードまたはフェールクローズモードにします。このコマンドは、インラインセットの [バイパス モード（Bypass Mode）] オプションが [バイパス（Bypass）] に設定されている場合にのみ使用できます。

デバイスを再起動するとインライン セットのフェールオープン モードが解除されるということに注意してください。

アクセス（Access）

設定（Configuration）

構文

```
configure bypass {open | close} {interface}
```

ここで、`interface` はインライン ペアのいずれかのハードウェア ポートの名前です。

例

```
> configure bypass open s1p1
```

high-availability

デバイスで高可用性のバイパスを無効にしたり、設定したりします。このコマンドは、NGIPSv、ASA FirePOWER、またはセカンダリ スタック メンバとして設定されているデバイスでは使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure high-availability {disable | bypass}
```

例

```
> configure high-availability disable
```

gui

デバイスの Web インターフェイス（システムのメジャーな更新時に表示される、簡潔なアップグレード Web インターフェイスなど）を有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure gui [enable | disable]
```

例

```
> configure gui disable
```

lcd

デバイスの正面の LCD ディスプレイを有効または無効にします。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure lcd {enable | disable}
```

例

```
> configure lcd disable
```

log-ips-connections

記録された侵入イベントに関連付けられている接続イベントのロギングを有効または無効にします。

アクセス（Access）

設定（Configuration）

構文

```
configure log-ips-connections {enable | disable}
```

例

```
> configure log-ips-connections disable
```

manager コマンド

`configure manager` コマンドは、管理元の Firepower Management Center へのデバイスの接続を設定します。

アクセス（Access）

設定（Configuration）

追加

管理元の Firepower Management Center からの接続を承認するようデバイスを設定します。このコマンドは、デバイスがアクティブに管理されていない場合にのみ機能します。

デバイスを Firepower Management Center に登録するには、常に一意の英数字の登録キーが必要です。ほとんどの場合は、登録キーと一緒にホスト名または IP アドレスを指定する必要があります。ただし、デバイスと Firepower Management Center が NAT デバイスによって分離されている場合は、登録キーと一緒に一意の NAT ID を入力し、ホスト名の代わりに `DONTRESOLVE` を指定します。

構文

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} regkey
[nat_id]
```

ここで、{hostname | IPv4_address | IPv6_address | DONTRESOLVE} は、このデバイスを管理する Firepower Management Center の DNS ホスト名、または IP アドレス（IPv4 または IPv6）を指定します。Firepower Management Center を直接アドレス指定できない場合は、DONTRESOLVE を使用します。DONTRESOLVE を使用する場合は nat_id が必要です。regkey は、デバイスを Firepower Management Center に登録するために必要な一意の英数字の登録キーです。nat_id は、Firepower Management Center とデバイス間の登録プロセスで使用される任意の英数字の文字列です。hostname が DONTRESOLVE に設定されている場合に必要です。

例

```
> configure manager add DONTRESOLVE abc123 efg456
```

削除

Firepower Management Center の接続情報をデバイスから削除します。このコマンドは、デバイスがアクティブに管理されていない場合のみ機能します。

構文

```
configure manager delete
```

例

```
> configure manager delete
```

mpls-depth

管理インターフェイスで MPLS レイヤの数を設定します。このコマンドは NGIPSv および ASA FirePOWER では使用できません。

アクセス（Access）

設定（Configuration）

構文

```
configure mpls-depth depth
```

ここで *depth* は 0～6 の数値です。

例

```
> configure mpls-depth 3
```

network コマンド

configure network コマンドは、デバイスの管理インターフェイスを設定します。

アクセス（Access）

設定（Configuration）

dns searchdomains

DNS 検索ドメインの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure network dns searchdomains {searchlist}
```

searchlist はカンマで区切られたドメインのリストです。

例

```
> configure network dns searchdomains foo.bar.com,bar.com
```

dns servers

DNS サーバの現行のリストを、コマンドで指定されたリストに置き換えます。

構文

```
configure nework dns servers {dnslist}
```

dnslist は、カンマで区切られた DNS サーバのリストです。

例

```
> configure network dns servers 10.123.1.10,10.124.1.10
```

hostname

デバイスのホスト名を設定します。

構文

```
configure network hostname {name}
```

name は新しいホスト名です。

例

```
> configure network hostname sfrocks
```

http-proxy

7000 & 8000 シリーズ および NGIPSv デバイスで、HTTP プロキシを設定します。コマンドを発行した後で、CLI はユーザに対して HTTP プロキシのアドレスとポート、プロキシの認証が必要かどうかを尋ねます。認証が必要な場合はプロキシのユーザ名、プロキシのパスワード、およびプロキシのパスワードの確認を入力するよう要求されます。

NGIPSv 上でこのコマンドを使用して、HTTP プロキシ サーバを設定し、仮想デバイスが動的解析のためにファイルを AMP クラウドへ送信できるようにします。

構文

```
configure network http-proxy
```

例

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address:
Enter HTTP Proxy Port:
Use Proxy Authentication? (y/n) [n]:
Enter Proxy Username:
Enter Proxy Password:
Confirm Proxy Password:
```

http-proxy-disable

7000 シリーズ、8000 シリーズ、または NGIPSv デバイスで、任意の HTTP プロキシの設定を削除します。

構文

```
configure network http-proxy-disable
```

例

```
> configure network http-proxy-disable
Are you sure that you wish to delete the current
http-proxy configuration? (y/n):
```

ipv4 delete

デバイスの管理インターフェイスの IPv4 設定を無効にします。

構文

```
configure network ipv4 delete [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv4 delete eth1
```

ipv4 dhcp

デバイスの管理インターフェイスの IPv4 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv4 dhcp [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

例

```
> configure network ipv4 dhcp
```

ipv4 manual

デバイスの管理インターフェイスの IPv4 設定を手動で設定します。

構文

```
configure network ipv4 manual ipaddr netmask [gw] [management_interface]
```

ここで *ipaddr* は IP アドレスで、*netmask* はサブネットマスク、*gw* はデフォルト ゲートウェイの IPv4 アドレスです。*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラット

フォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは**eth0**、オプションのイベントインターフェイスでは**eth1** です。

例

```
> configure network ipv4 manual 10.123.1.10 255.255.0.0 10.123.1.1
```

ipv6 delete

デバイスの管理インターフェイスの IPv6 設定を無効にします。

構文

```
configure network ipv6 delete [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス IDは、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 delete
```

ipv6 dhcp

デバイスの管理インターフェイスの IPv6 設定を DHCP に設定します。管理インターフェイスは DHCP サーバと通信して、設定情報を取得します。

構文

```
configure network ipv6 dhcp [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。DHCP はデフォルトの管理インターフェイスでのみサポートされているため、この引数を使用する必要はありません。

例

```
> configure network ipv6 dhcp
```

ipv6 manual

デバイスの管理インターフェイスの IPv6 設定を手動で設定します。

構文

```
configure network ipv6 manual ip6addr/ip6prefix [ip6gw] [management_interface]
```

ここで *ip6addr*/*ip6prefix* は IP アドレスとプレフィックス長、*ip6gw* はデフォルト ゲートウェイの IPv6 アドレスを表します。*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 manual 2001:DB8:3ffe:1900:4545:3:200:f8ff:fe21:67cf 64
```

ipv6 router

デバイスの管理インターフェイスの IPv6 設定をルータに設定します。管理インターフェイスは IPv6 ルータと通信して、設定情報を取得します。

構文

```
configure network ipv6 router [management_interface]
```

ここで、*management_interface* は管理インターフェイス ID です。インターフェイスを指定しない場合、このコマンドはデフォルトの管理インターフェイスを設定します。このパラメータは、**configure management-interface** コマンドを使って複数の管理インターフェイスを有効にする場合にのみ必要です。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。他のプラットフォームではこのパラメータを指定しないでください。管理インターフェイス ID は、デフォルト管理インターフェイスでは **eth0**、オプションのイベント インターフェイスでは **eth1** です。

例

```
> configure network ipv6 router
```

management-interface disable

管理インターフェイスを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス を参照してください。

例

```
> configure network management-interface disable eth1
```

management-interface disable-event-channel

指定された管理インターフェイスでイベント トラフィック チャネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable-event-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス を参照してください。

例

```
> configure network management-interface disable-event-channel eth1
```

management-interface disable-management-channel

指定された管理インターフェイスで管理トラフィック チャネルを無効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface disable-management-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス を参照してください。

例

```
> configure network management-interface disable-management-channel eth1
```

management-interface enable

指定した管理インターフェイスを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable ethn
```

n は、有効にする管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。

デバイスを管理する場合、Firepower Management Center 管理インターフェイスには 2 つの別個のトラフィック チャネルがあります。管理トラフィック チャネルはすべての内部トラフィック（デバイスの管理に固有のデバイス間トラフィックなど）を伝送し、イベント トラフィック チャネルはすべてイベント トラフィック（Web イベントなど）を伝送します。必要に応じて、Management Center で個別のイベント専用インターフェイスを設定し、イベント トラフィックを処理することもできます（Firepower Management Center Web インタ フェースで、この設定が実行されていることを確認してください）。イベント専用インターフェイスは 1 つだけ設定できます。イベント トラフィックは大量の帯域幅を使用する可能性があるので、管理トラフィックからイベント トラフィックを分離することで、Management Center のパフォーマンスを向上させることができます。

デフォルトの eth0 インターフェイスには、デフォルトで管理とイベント チャンネルの両方が含まれています。必要に応じて、イベント専用インターフェイスとして eth0 インターフェイスを有効にできます。可能であれば、デバイス イベント インターフェイスと Firepower Management Center イベント インターフェイスの間で、イベント トラフィックが送信されます。イベント ネットワークがダウンすると、イベント トラフィックは、デフォルトの管理インターフェイスに戻ります。可能な場合には別個のイベント インターフェイスが使用されますが、管理インターフェイスが常にバックアップとなります。

管理インターフェイスを有効にすると、管理とイベント チャンネルの両方がデフォルトで有効にされます。管理チャネルとイベント チャネルの両方にデフォルト管理インターフェイスを使

用することをお勧めします。その後、別個のイベント専用インターフェイスを有効にします。Firepower Management Center イベント専用インターフェイスは管理チャネルのトラフィックを受け入れることができないので、デバイス イベント インターフェイスで管理チャネルを単に無効にしてください。

configure network {**ipv4** | **ipv6**} **manual** コマンドを使用して、管理インターフェイスのアドレスを設定します。

例

```
> configure network management-interface enable eth1
> configure network management-interface disable-management-channel eth1
```

management-interface enable-event-channel

指定された管理インターフェイスでイベント トラフィック チャネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable-event-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス を参照してください。

例

```
> configure network management-interface enable-event-channel eth1
```

management-interface enable-management-channel

指定された管理インターフェイスで管理トラフィック チャネルを有効にします。複数の管理インターフェイスは、8000 シリーズ デバイスおよび ASA 5585-X with FirePOWER サービスでのみサポートされています。

構文

```
configure network management-interface enable-management-channel ethn
```

n は、設定する管理インターフェイスの数です。**eth0** デフォルト管理インターフェイスです。**eth1** はオプションのイベント インターフェイスです。シスコでは、管理チャネルとイベント

チャネルの両方を有効にして、eth0デフォルト管理インターフェイスを有効のままにすることを推奨しています。Firepower Management Center および管理対象デバイスで個別のイベント インターフェイスを使用する方法の詳細については、管理インターフェイス を参照してください。

例

```
> configure network management-interface enable-management-channel eth1
```

management-interface tcpport

管理用の TCP ポートの値を変更します。

構文

```
configure network management-interface tcpport port
```

port は設定する管理ポートの値です。

例

```
> configure network management-interface tcpport 8500
```

management-port

デバイスの TCP 管理ポートの値を設定します。

構文

```
configure network management-port number
```

number は設定する管理ポートの値を表します。

例

```
> configure network management-port 8500
```

static-routes ipv4 add

指定した管理インターフェイスの IPv4 スタティック ルートを追加します。

構文

```
configure network static-routes ipv4
add interface destination netmask gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、netmask はネットワーク マスク アドレス、gateway は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4
add eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv4 delete

指定した管理インターフェイスの IPv4 スタティック ルートを削除します。

構文

```
configure network static-routes ipv4
delete interface destination netmask gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、netmask はネットワーク マスク アドレス、gateway は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv4
delete eth1 10.115.24.0 255.255.255.0 10.115.9.2
```

static-routes ipv6 add

指定した管理インターフェイスの IPv6 スタティック ルートを追加します。

構文

```
configure network static-routes ipv6
add interface destination prefix gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、prefix は IPv6 プレフィックス長、gateway は追加するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6
add eth1 2001:DB8:3ffe:1900:4545:3:200: f8ff:fe21:67cf 64
```

static-routes ipv6 delete

指定した管理インターフェイスの IPv6 スタティック ルートを削除します。

構文

```
configure network static-routes ipv6
delete interface destination prefix gateway
```

interface は管理インターフェイス、destination は宛先 IP アドレス、prefix は IPv6 プレフィックス長、gateway は削除するゲートウェイ アドレスです。

例

```
> configure network static-routes ipv6
delete eth1 2001:DB8:3ffe:1900:4545:3:200:f8ff: fe21:67cf 64
```

password

現行のユーザは、自身のパスワードを変更することができます。コマンドを発行すると、CLI は現在の（古い）パスワードを入力するようユーザに要求し、その後で新しいパスワードを 2 回入力するよう要求します。

アクセス（Access）

基本

構文

```
configure password
```

例

```
> configure password
Enter current password:
Enter new password:
Confirm new password:
```

スタッキングの無効化

7000 および 8000 シリーズ のデバイスでは、次のデバイスに存在するスタック構成はすべて削除されます。

- プライマリとして設定されているデバイスでは、スタックは完全に削除されます。
- セカンダリとして設定されているデバイスでは、そのデバイスはスタックから削除されます。

このコマンドは、NGIPSv または ASA FirePOWER モジュールでは使用できません。また、これを使用してデバイスの高可用性ペアを解除することはできません。

スタッキング階層の上位アプライアンスとの通信を確立できない場合は、このコマンドを使用します。Firepower Management Center を通信で使用できる場合は、代わりに Firepower Management Center の Web インターフェイスを使用するよう伝えるメッセージが表示されます。同様に、プライマリ デバイスを使用できる場合に、セカンダリとして設定されているデバイス上で `stacking disable` を入力すると、プライマリ デバイスからコマンドを入力するよう伝えるメッセージが表示されます。

アクセス（Access）

設定（Configuration）

構文

```
configure stacking disable
```

例

```
> configure stacking disable
```

user コマンド

NGIPSv でのみ使用できます。`configure user` コマンドは、デバイスのローカル ユーザ データベースを管理します。

アクセス（Access）

設定（Configuration）

アクセス

指定したユーザのアクセス レベルを変更します。このコマンドは、指定されたユーザが次にログインするときに有効になります。

構文

```
configure user access username [basic | config]
```

username は、アクセスを変更するユーザの名前を表します。`basic` は basic アクセスを、`config` は configuration アクセスを表します。

例

```
> configure user access jdoe basic
```

追加

指定された名前とアクセス レベルを使用して新しいユーザを作成します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user add username [basic | config]
```

ここで、username は新しいユーザの名前を指定します。basic は基本アクセス、config は設定アクセスを表します。

例

```
> configure user add jdoe basic
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

aging

ユーザのパスワードに有効期限を設定します。

構文

```
configure user aging username max_days warn_days
```

ここで、username はユーザの名前、max_days はパスワードが有効な最大日数、warn_days は有効期限が切れる前にユーザがパスワードを変更するために確保されている日数を表します。

例

```
> configure user aging jdoe 100 3
```

削除

ユーザとユーザのホーム ディレクトリを削除します。

構文

```
configure user delete username
```

username はユーザの名前を表します。

例

```
> configure user delete jdoe
```

disable

ユーザを無効にします。無効なユーザはログインできません。

構文

```
configure user disable username
```

username はユーザの名前を表します。

例

```
> configure user disable jdoe
```

enable

ユーザを有効にします。

構文

```
configure user enable username
```

username はユーザの名前を指定します。

例

```
> configure user enable jdoe
```

forcereset

ユーザが次にログインするときに、パスワードの変更を要求します。ユーザがログインしてパスワードを変更すると、強度のチェックが自動的に有効になります。

構文

```
configure user forcereset username
```

username はユーザの名前を表します。

例

```
> configure user forcereset jdoe
```

maxfailedlogins

指定したユーザが、ログインで失敗できる最大回数を設定します。

構文

```
configure user maxfailedlogins username number
```

username はユーザの名前、*number* は、ログインで失敗できる最大回数を表します。

例

```
> configure user maxfailedlogins jdoe 3
```

password

ユーザのパスワードを設定します。このコマンドでは、ユーザのパスワードを入力するよう要求されます。

構文

```
configure user password username
```

username はユーザの名前を表します。

例

```
> configure user pasword jdoe
Enter new password for user jdoe:
Confirm new password for user jdoe:
```

strengthcheck

ユーザのパスワードに対する強度の要件を有効または無効にします。ユーザパスワードの有効期限が切れた場合、または configure user forcereset コマンドを使用した場合は、ユーザが次にログインしたときにこの要件が自動的に有効になります。

構文

```
configure user strengthcheck username {enable | disable}
```

username はユーザの名前を表します。`enable` は指定されたユーザのパスワードの要件を設定し、`disable` は、指定されたユーザのパスワードの要件を削除します。

例

```
> configure user strengthcheck jdoe enable
```

unlock

ログイン失敗の最大数を超過したユーザをロック解除します。

構文

```
configure user unlock username
```

username はユーザの名前を表します。

例

```
> configure user unlock jdoe
```

vmware-tools

NGIPSv での VMware Tools の機能を有効または無効にします。このコマンドは、NGIPSv のみで使用できます。

VMwareツールは、仮想マシンのパフォーマンスを向上させるためのユーティリティスイートです。これらのユーティリティを使用すると、VMware 製品の便利な機能をすべて活用できます。このシステムは、すべての仮想アプライアンスで次のプラグインをサポートします。

- guestInfo
- powerOps
- timeSync
- vmbackup

VMware ツールおよびサポートされるプラグインの詳細については、VMware の Web サイト（http://www.vmware.com）を参照してください。

アクセス（Access）

基本

構文

```
configure vmware-tools [enable | disable]
```

例

```
> configure vmware-tools enable
```

system コマンド

system コマンドを使用して、システム全体のファイルおよびアクセス コントロールの設定を管理することができます。Configuration CLI アクセス権を持つユーザのみが、システム モードでコマンドを発行できます。

アクセス制御コマンド

`system access-control` コマンドは、ユーザがデバイス上でアクセス制御設定を管理できるようにします。

アクセス（Access）

設定（Configuration）

archive

現在展開されているアクセス コントロール ポリシーをテキスト ファイルとして `/var/common` に保存します。

構文

```
system access-control archive
```

例

```
> system access-control archive
```

clear-rule-counts

アクセス コントロール ルールのヒット数を 0 にリセットします。

構文

```
system access-control clear-rule-counts
```

例

```
> system access-control clear-rule-counts
```

rollback

これまでに導入されたアクセス制御設定に対して、システムの復帰を行います。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

構文

```
system access-control rollback
```

例

```
> system access-control rollback
```

コンプライアンス コマンド

コンプライアンス（compliance）コマンドは、デバイスのセキュリティ認定コンプライアンス モードの表示、設定を行います。

注意 この設定を有効にすると、無効化することはできません。無効化する必要がある場合は、サポート窓口にご連絡ください。

アクセス（Access）

設定（Configuration）

enable cc

デバイスのセキュリティ認定準拠をコモン クライテリア（CC）モードに設定します。

注意 この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

構文

```
system compliance enable cc
```

例

```
> system compliance enable cc
```

enable ucapl

デバイスのセキュリティ認定準拠を統合機能承認取得済み製品リスト（UCAPL）モードに設定します。

⚠

注意 この設定を有効にした後は、無効にすることはできません。無効にする必要がある場合は、サポートにお問い合わせください。

構文

```
system compliance enable ucapl
```

例

```
> system compliance enable ucapl
```

show

デバイスの現在のセキュリティ認定のコンプライアンス モードを表示します。

構文

```
system compliance show
```

例

```
> system compliance show
```

disable-http-user-cert

システム上に存在するすべての HTTP ユーザ証明書を削除します。

アクセス（Access）

設定（Configuration）

構文

```
system disable-http-user-cert
```

例

```
> system disable-http-user-cert
```

file コマンド

system file コマンドを使用すると、ユーザは、デバイス上の common ディレクトリにあるファイルを管理することができます。

アクセス（Access）

設定（Configuration）

copy

FTP を使用して、ログイン ユーザ名を使用しているホスト上のリモート ロケーションへファイルを転送します。ローカル ファイルは common ディレクトリに配置する必要があります。

構文

```
system file copy hostname username path filenames filenames ...
```

hostname はターゲットのリモート ホストの名前または IP アドレスを表します。username はリモート ホスト上のユーザの名前、path はリモート ホスト上の宛先パス、filenames は転送するローカル ファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file copy sfrocks jdoe /pub *
```

削除

common ディレクトリから、指定したファイルを削除します。

構文

```
system file delete filenames filenames ...
```

filenames は削除するファイルを指定します。複数のファイル名はスペースで区切って指定します。

例

```
> system file delete *
```

list

ファイル名が指定されていない場合は、common ディレクトリ内のすべてのファイルについて変更の時刻、サイズ、およびファイル名が表示されます。ファイル名が指定されている場合

は、指定されたファイル名と一致したファイルで、変更の時刻、サイズ、およびファイル名が表示されます。

構文

```
system file list filenames
```

filenames は表示するファイルを表します。複数のファイル名はスペースで区切って指定します。

例

```
> system file list
```

secure-copy

SCP を使用して、ログイン ユーザ名でホストのリモート ロケーションにファイルを転送します。ローカル ファイルは、/var/common ディレクトリに配置する必要があります。

構文

```
system file secure-copy hostname username path filenames filenames ...
```

hostname では、対象のリモート ホストの名前または ip アドレスを指定します。*username* では、リモート ホストのユーザ名を指定します。*path* では、リモート ホストの宛先パスを指定します。*filenames* では、転送するローカル ファイルを指定します。ファイル名はスペースで区切ります。

例

```
> system file secure-copy 10.123.31.1 jdoe /tmp *
```

generate-troubleshoot

シスコが解析に使用するトラブルシューティング データを生成します。

アクセス（Access）

設定（Configuration）

構文

```
system generate-troubleshoot
```

この構文は、どのトラブルシューティングデータを表示するかを指定するための、オプションのパラメータのリストを表示します。

例

```
> system generate-troubleshoot
```

ldapsearch

ユーザが、指定されたLDAPサーバのクエリを実行できるようにします。すべてのパラメータが必須であることに注意してください。

アクセス（Access）

設定（Configuration）

構文

```
system ldapsearch host port baseDN userDN basefilter
```

hostはLDAPサーバのドメイン、portはLDAPサーバのポート、baseDNは検索するDN（識別名）、userDNはLDAPディレクトリへバインドするユーザのDN、basefilterは検索するレコードを表します。

例

```
> system ldapsearch ldap.example.com 389 cn=users,

dc=example,dc=com cn=user1,cn=users,dc=example,dc=com, cn=user2
```

lockdown-sensor

`expert` コマンドを削除し、デバイス上のbashシェルへアクセスします。

⚠

注意 このコマンドは、サポートからのホットフィックスがない場合は取り消すことはできません。使用には注意が必要です。

アクセス（Access）

設定（Configuration）

構文

```
system lockdown-sensor
```

例

```
> system lockdown-sensor
```

nat rollback

以前に適用していたNATの設定に、システムを戻します。このコマンドはNGIPSvまたはASA FirePOWER では使用できません。このコマンドをスタックまたは高可用性ペアのデバイスで使用することはできません。

アクセス（Access）

設定（Configuration）

構文

```
system nat rollback
```

例

```
> system nat rollback
```

reboot

デバイスをリブートします。

アクセス（Access）

設定（Configuration）

構文

```
system reboot
```

例

```
> system reboot
```

restart

デバイスのアプリケーションを再起動します。

アクセス（Access）

設定（Configuration）

構文

```
system restart
```

例

```
> system restart
```

support コマンド

`system support` コマンドを使用することで、デバイス上の特殊な SSL ClientHello 処理を管理できます。

アクセス（Access）

設定（Configuration）

ssl-client-hello-display

SSL ハンドシェイク時に ClientHello メッセージを処理するための現在の設定を表示します。これらの設定の説明については、`ssl-client-hello-enabled` および `ssl-client-hello-tuning` コマンドを参照してください。

アクセス（Access）

基本

構文

```
system support ssl-client-hello-display
```

例

```
> system support ssl-client-hello-display
```

ssl-client-hello-enabled

SSL ハンドシェイク時に ClientHello メッセージの特殊な処理を制御します。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないでください**。

従来型デバイスのコマンド ライン リファレンス

アクセス（Access）

設定（Configuration）

構文

```
system support ssl-client-hello-enabled setting {true | false}
```

Setting に指定できる値は次のとおりです。

feature
ClientHello メッセージのすべての特殊な処理を制御します。

curves
Firepower システムでサポートされていない楕円曲線の削除を制御します。

- `true`（有効）：サポートされていないすべての楕円曲線を ClientHello メッセージから削除し、トラフィックの復号の確率が向上します。`extensions` 設定を有効にする必要もあります。
- `false`（無効）：ClientHello メッセージ内のサポートされていない楕円曲線を保持し、トラフィックの復号の確率が低下します。

ciphers
Firepower システムでサポートされていない暗号スイートの削除を制御します。

- `true`（有効）：サポートされていない暗号スイートを ClientHello メッセージから削除し、トラフィックの復号の確率が向上します。
- `false`（無効）：ClientHello メッセージ内のサポートされていない暗号スイートを保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで多数の `Unsupported` エラーや `Unknown Cipher` エラーが発生する可能性があります。

内線番号

復号を妨げる TLS 拡張の削除を制御します。

- `true`（有効）：復号を妨げる TLS 拡張を特定し、ClientHello メッセージから削除します。**curves**、**session_ticket**、および **alpn** を有効にする場合、この値を指定する必要があります。
- `false`（無効）：ClientHello メッセージ内のすべての TLS 拡張を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで `Unknown Session` エラーが発生する可能性があります。

session_ticket
ClientHello メッセージの SessionTicket 拡張の処理を制御します。システムが着信 ClientHello メッセージ内の SessionTicket 値をキャッシュされたセッション データと照合できる場合、クライアントとサーバで完全な SSL ハンドシェイクが実行されなくてもセッションを再開できます。

従来型デバイスのコマンド ライン リファレンス

- `true`（有効）：認識されない SessionTicket 値を ClientHello メッセージから削除します。これにより、再開されたセッションでトラフィックの復号の確率が向上します。`extensions` 設定を有効にする必要もあります。
- `false`（無効）：ClientHello メッセージ内のすべての SessionTicket 値を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで `Uncached Session` エラーが発生する可能性があります。

session_id

ClientHello メッセージのセッション識別子要素の処理を制御します。システムが着信 ClientHello メッセージ内のセッション識別子をキャッシュされたセッションデータと照合できる場合、クライアントとサーバで完全な SSL ハンドシェイクが実行されなくてもセッションを再開できます。

- `true`（有効）：認識されないセッション識別子値を ClientHello メッセージから削除します。これにより、再開されたセッションでトラフィックの復号の確率が向上します。
- `false`（無効）：ClientHello メッセージ内のすべてのセッション識別子値を保持します。これによりトラフィックの復号の確率が低下し、関連する接続イベントの SSL Flow Error フィールドで `Uncached Session` エラーが発生する可能性があります。

alpn

復号できない ALPN プロトコル値、特に SPDY および HTTP2 プロトコルの削除を制御します。

- `true`（有効）：クライアントが SPDY または HTTP2 セッションを確立することを禁止し、トラフィックの復号および検査の確率が向上します。`extensions` 設定を有効にする必要もあります。
- `false`（無効）：クライアントがサーバと SPDY または HTTP2 セッションを確立することを許可し、トラフィックの復号および検査の確率が低下します。

compression

ClientHello メッセージからの TLS 圧縮要求の削除を制御します。

- `true`（有効）：クライアントがサーバと TLS 圧縮セッションを確立することを禁止します。
- `false`（無効）：クライアントがサーバと TLS 圧縮セッションを確立することを許可します。これによりセッションのトラフィックの復号が妨げられ、関連する接続イベントの SSL Flow Error フィールドで `Compression Used` エラーが発生する可能性があります。

例

```
> system support ssl-client-hello-enabled feature false
```

ssl-client-hello-force-reset

デフォルト値に処理するClientHelloメッセージの設定可能な設定をリセットします。システムはユーザの確認を必要とせず続行します。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス（Access）

設定（Configuration）

構文

```
system support ssl-client-hello-force-reset
```

例

```
> system support ssl-client-hello-force-reset
```

ssl-client-hello-reset

デフォルト値に処理するClientHelloメッセージの設定可能な設定をリセットします。システムは、続行する前にユーザの確認を必要とします。

⚠

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス（Access）

設定（Configuration）

構文

```
system support ssl-client-hello-reset
```

例

```
> system support ssl-client-hello-reset
```

ssl-client-hello-tuning

SSLハンドシェイク時に管理対象デバイスがClientHelloメッセージをどのように変更するか調整できます。このコマンドは、ClientHelloメッセージで許可される暗号スイート、楕円曲線、および拡張のデフォルト リストを調整します。このコマンドは、許可される値のデフォルト

従来型デバイスのコマンド ライン リファレンス

リストにエントリを追加するか、許可される値のデフォルトリストからエントリを削除するだけです。デフォルト リストは上書きされません。

注意 サポートからの指示がない限り、このコマンドは使用**しないで**ください。

アクセス（Access）

設定（Configuration）

構文

```
system support ssl-client-hello-tuning setting value
```

value 要素は値のカンマ区切りのリストをサポートします。*setting* および *value* 要素の設定可能な値には次が含まれます。

設定	システムのアクション	値
`ciphers_allow`	ClientHello メッセージで指定された暗号スイートを許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された暗号スイートを保持します。	IANA の Web サイトから個々の暗号スイートの数を取得します。 https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-4 IANA は 16 進数の値を提供します。このコマンドを使用してそれらを 10 進数に変換します。
`ciphers_remove`	ClientHello メッセージで指定された暗号スイートを拒否します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージから指定された暗号スイートを削除します。	

設定	システムのアクション	値
curves_allow	ClientHello メッセージで指定された楕円曲線を許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された楕円曲線を保持します。	IANA の Web サイトから曲線の数を取得します。https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml#tls-parameters-8
curves_remove	ClientHello メッセージで指定された楕円曲線を拒否します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージから指定された楕円曲線を削除します。	
extensions_allow	ClientHello メッセージで指定された拡張を許可します。このコマンドを使用すると、システムは変更するすべての ClientHello メッセージで指定された拡張を保持します。	IANA の Web サイトから拡張の数を取得します。https://www.iana.org/assignments/tls-extensiontype-values/tls-extensiontype-values.xhtml
extensions_remove	ClientHello メッセージで指定された楕円曲線を拒否します。システムは変更するすべての ClientHello メッセージから指定された拡張を削除します。デフォルトでは、システムは拡張 22、23、および 30032 を拒否します。	

例

```
> system support ssl-client-hello-tuning ciphers_allow 4,7,16,22
```

shutdown

デバイスをシャットダウンします。このコマンドは ASA FirePOWER モジュールでは使用できません。

従来型デバイスのコマンド ライン リファレンス

アクセス（**Access**）

設定（Configuration）

構文

```
system shutdown
```

例

```
> system shutdown
```