d - r

debug

特定の機能のデバッグ メッセージを表示するには、**debug** コマンドを使用します。デバッグ メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。すべてのデバッグ コマンドをオフにするには、**no debug all** を使用します。

debug *feature* ［*subfeature*］［*level*］
no debug *feature* ［*subfeature*］

構文の説明

feature	デバッグをイネーブルにする機能を指定します。使用可能な機能を表示するには、**debug ?** コマンドを使用して CLI ヘルプを表示します。
subfeature	（オプション）機能によっては、1 つ以上のサブ機能のデバッグ メッセージをイネーブルにできます。使用可能なサブ機能を表示するには ? を使用します。
level	（オプション）デバッグ レベルを指定します。このレベルは、一部の機能で使用できない場合があります。使用可能なレベルを表示するには ? を使用します。

コマンド デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
7.2	このコマンドは、パスモニタリングのデバッグを含めるように変更されました。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

デバッグ出力は、CLIセッションでのみ表示できます。出力は、コンソール ポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の 脅威に対する防御 CLI からの出力を確認することもできます。

例

次の例では、DNS デバッグを有効にし、診断 CLI でメッセージを生成するアクションを実行します。デバッグメッセージは、「ERROR: % Invalid Hostname」というメッセージに続いて開始されます。Enter を押してプロンプトを表示します。次の例で、これらのデバッグメッセージが **show console-output** のディスプレイにどのように表示されるかを示します。

```
> debug dns
debug dns enabled at level 1.

> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower# ping www.example.com
                ^
ERROR: % Invalid Hostname
firepower# DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled
DNS: get global group DefaultDNS handle 1fa0b047
DNS: Resolve request for 'www.example.com' group DefaultDNS
DNS: No interfaces enabled

firepower# (press Ctrl+a, then d, to return to the regular CLI.)

Console connection detached.
> show console-output
... (output redacted)...
Message #75 : DNS: get global group DefaultDNS handle 1fa0b047
Message #76 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #77 : DNS: No interfaces enabled
Message #78 : DNS: get global group DefaultDNS handle 1fa0b047
Message #79 : DNS: Resolve request for 'www.cisco.com' group DefaultDNS
Message #80 : DNS: No interfaces enabled
```

関連コマンド

Command	説明
show debug	現在アクティブなデバッグ設定を示します。
undebug	ある機能のデバッグを無効にします。このコマンドは **no debug** の同意語です。

debug packet-condition

デバッグする必要があるフローにフィルタを適用するには、**debug packet-condition** コマンドを使用します。フローのフィルタを削除するには、このコマンドの **no** 形式を使用します。フローのすべてのフィルタをオフにする場合、**no debug packet-condition** を使用します。

debug packet-condition [**position** *<line>*] **match** *<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* [*<src_operator> <ports> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}*] [*<dest_operator> <ports>*] [*<icmp_type>* | *<icmp6_type>*] [*connection <connection-id>*] [*unidirectional*]

構文の説明

position *<line>*	既存のフィルタのリストでフィルタを配置する位置を指定します。 *<line>* は番号を示します。
match*<proto> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}*	フィルタの一致条件を指定します。 *<proto>* はプロトコルを示します。 *{any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}* は IP アドレスオプションを示します。
<src_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}	（オプション）送信元のポートまたは IP アドレスを指定します。
<dest_operator><port> {any|any4|any6|host <ip>|<ipv4>|<ipv4_mask>|<ipv6>/<prefixlen>}	（オプション）宛先のポートまたはIPアドレスの詳細を指定します。
<icmp_type>|<icmp6_type>	（オプション）接続の ICMP のタイプを指定します。
connection <connection-id>	（オプション）進行中の接続の接続 ID を指定します。
unidirectional	（オプション）指定した方向のパケットに対してのみデバッグを実行することを指定します。変数が指定されていない場合、デフォルトの動作は双方向であり、トラフィックは接続の順方向と逆方向の両方のフローと照合されます。

コマンド デフォルト

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。

リリース	変更内容
6.5	**debug packet condition** コマンドが **debug packet-condition** に変更されました。
6.6	進行中の接続をサポートするようにコマンド **debug packet-condition** が強化されました。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

デバッグ出力は、CLIセッションでのみ表示できます。出力は、コンソール ポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の 脅威に対する防御 CLI からの出力を確認することもできます。

例

次に、デバッグする必要があるフローにフィルタを設定する方法の例を示します。

```
> debug packet-condition position 7 match tcp 1.2.3.0 255.255.255.0 any4
> debug packet-condition match tcp 1.2.3.0 255.255.255.0 eq www any4 unidirectional
> debug packet-condition match connection 70856531
> no debug packet-condition match tcp 1.2.3.0 255.255.255 eq www unidirectional
```

関連コマンド

Command	説明
debug packet-start	デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。
debug packet-stop	デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。

debug packet-module

デバッグメッセージを送信する各モジュールのレベルを設定するには、**debug packet-module** コマンドを使用します。レベルは 0（緊急）ー 7（デバッグ）の範囲で設定できます。レベルを設定すると、シビラティ（重大度）が同等以上のすべてのメッセージがログに記録されます。現在、サポートされているのは、DAQ、PDTS、ACL、およびSnortモジュールのみです。

debug packet-module [**acl** | **all** | **daq** | **pdts** | **snort-engine** | **snort-fileprocessor** | **snort-firewall**] < *0* ～ *7* >

構文の説明

acl	パケット処理パスのアクセス コントロール ポリシーを選択します。
all	パケット処理パスのすべてのモジュールを選択します。
daq	パケット処理パスの DAQ 情報を選択します。
pdts	パケット処理パスの PDTS（Snort へのデータプレーン送信/受信キュー）通信を選択します。
snort-engine	パケット処理パスの Snort 情報を選択します。
snort-fileprocessor	パケット処理パスの Snort ファイルプロセッサ情報を選択します。
snort-firewall	パケット処理パスの Snort ファイアウォール情報を選択します。

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。
6.5	**debug packet** コマンドが **debug packet-module** に変更されました。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

デバッグ出力は、CLIセッションでのみ表示できます。出力は、コンソールポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の 脅威に対する防御 CLI からの出力を確認することもできます。

例

次に、パケット処理パスの DAQ 情報にレベルを設定する例を示します。

```
> debug packet daq 6
```

関連コマンド

Command	説明
debug packet-start	デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。
debug packet-stop	デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。

debug packet-module trace

モジュールレベルのパケットトレースを有効にするには、**debug packet-module trace** コマンドを使用します。

debug packet-module trace

コマンド履歴

リリース	変更内容
6.6	このコマンドが導入されました。

使用上のガイドライン

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. したがって、**debug** コマンドを使用するのは、特定の問題のトラブルシューティング時か、または Cisco Technical Assistance Center（TAC）とのトラブルシューティング セッション時に限定してください。さらに、**debug**コマンドは、ネットワークトラフィックが少なく、ユーザも少ないときに使用することを推奨します。デバッギングをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が低くなります。

デバッグ出力は、CLIセッションでのみ表示できます。出力は、コンソールポートに接続したときか、または診断 CLI（**system support diagnostic-cli** と入力）で直接入手できます。また、**show console-output** コマンドを使用して、通常の 脅威に対する防御 CLI からの出力を確認することもできます。

例

次に、モジュールレベルのパケットトレースを有効にする例を示します。

```
> debug packet-module trace
```

次に、**debug packet-module trace** コマンドの出力例を示します。

```
ID          | Details                                                                  | Time
(ns)
------------ -------------------------------------------------------------------------
------------------------------
6525759     | TCP        74.125.24.156      : 443   -> 192.168.0.31      : 58280 |
19-02-2020 06:48:43.050675868
```

さらに、次のコマンドを使用して、パケットの詳細を取得できます。

```
> show packet debugs module trace packet-id 6525759

Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.050675868(ns)
****************************************
Module: translate
Entry Time: 19-02-2020 06:48:43.050684452(ns)
****************************************
Module: inspect_snort
Entry Time: 19-02-2020 06:48:43.050688028(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.050691843(ns)
```

```
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051417112(ns)
****************************************
Module: pdts
Entry Time: 19-02-2020 06:48:43.051421642(ns)
****************************************
Module: tcp-normalizer
Entry Time: 19-02-2020 06:48:43.051424980(ns)
****************************************
Module: adjacency
Entry Time: 19-02-2020 06:48:43.051438331(ns)
****************************************
Module: fragment
Entry Time: 19-02-2020 06:48:43.051442861(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750763893(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750815391(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750831365(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750843286(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750889778(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750911474(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.750942230(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750986576(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.750999689(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751020193(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751051425(ns)
****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751075029(ns)
****************************************
Module: snort_firewall
Entry Time: 19-02-2020 06:48:43.751084804(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751099348(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751118421(ns)
****************************************
Module: snort_engine
Entry Time: 19-02-2020 06:48:43.751137018(ns)
****************************************
```

```
Module: daq
Entry Time: 19-02-2020 06:48:43.751152753(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751164197(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751177072(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751186609(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751203775(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751224517(ns)
****************************************
Module: daq
Entry Time: 19-02-2020 06:48:43.751236677(ns)
****************************************
```

関連コマンド

Command	説明
show packet debugs module trace	各モジュールから収集されたすべてのデバッグトレースのリストを表示します。
debug packet-start	デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。
debug packet-stop	デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。

debug packet-start

パケットのデバッグを開始し、デバッグログデータベースへのデバッグログの書き込みを開始するには、**debug packet-start** コマンドを使用します。

debug packet-start

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。
6.5	このコマンドは、**debug packet start** から **debug packet-start** に変更されました。

使用上のガイドライン

debug packet-start は、デバッグログデータベースへの接続を開きます。このコマンドが呼び出されない限り、デバッグログはデータベースに書き込まれません。

例

次に、パケットのデバッグを開始する例を示します。

```
> debug packet-start
```

関連コマンド

Command	説明
debug packet-stop	デバッグログデータベースへの接続を閉じ、データベースへのデバッグログの書き込みを停止します。

debug packet-stop

パケットのデバッグを停止し、デバッグログデータベースへのデバッグログの書き込みを停止するには、**debug packet-stop** コマンドを使用します。

debug packet-stop

コマンド履歴

リリース	変更内容
6.4	このコマンドが導入されました。
6.5	このコマンドは、**debug packet stop** から **debug packet-stop** に変更されました。

使用上のガイドライン

debug packet-stop は、デバッグログデータベースへの接続を閉じます。

例

次に、パケットのデバッグを停止する例を示します。

```
> debug packet-stop
```

関連コマンド

Command	説明
debug packet-start	デバッグログデータベースへの接続を開き、データベースへのデバッグログの書き込みを開始します。

delete

フラッシュメモリからファイルを削除するには、**delete** コマンドを使用します。

delete /noconfirm ［**/recursive**］［**/replicate**］［**disk0:** | **disk***n***:** | **flash:**］[*path/*] *filename*

構文の説明

/noconfirm	確認のためのプロンプトを表示しません。
/recursive	（任意）すべてのサブディレクトリの指定されたファイルを再帰的に削除します。
/replicate	（オプション）スタンバイ ユニットの指定されたファイルを削除します。
disk0:	（オプション）内部のフラッシュ メモリを指定します。
disk*n***:**	（任意）オプションの外部フラッシュドライブを示します。n でドライブ番号を指定します。通常は disk1 です。
filename	削除するファイルの名前を指定します。
flash:	（オプション）内部のフラッシュ メモリを指定します。このキーワードは **disk0** と同じです。
path/	（任意）ファイルのパスに指定します。

コマンド デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

パスを指定しない場合は、現在の作業ディレクトリからファイルが削除されます。ファイルの削除では、ワイルドカードがサポートされています。

例

次に、現在の作業ディレクトリから test.cfg という名前のファイルを削除する例を示します。

```
> delete /noconfirm test.cfg
```

関連コマンド

Command	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	現在のディレクトリ内のファイルを一覧表示します。
rmdir	ファイルまたはディレクトリを削除します。

dig

完全修飾ドメイン名の IP アドレスを検索するには、**dig** コマンドを使用します。

dig *hostname*

構文の説明

hostname	IP アドレスを検索するホストの完全修飾ドメイン名。たとえば、www.example.com などです。

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。このコマンドは、**nslookup** コマンドに置き換えられました。

使用上のガイドライン

完全修飾ドメイン名を許可するコマンドの中には、管理インターフェイス用に設定されたDNSサーバーを使用して完全修飾ドメイン名からIPアドレスを検索できないものがあります。データインターフェイスを通過するコマンド用にDNSサーバーが設定されていない場合は、**dig** コマンドを使用して IP アドレスを特定し、そのコマンドで IP アドレスを使用します。

dig コマンドは、管理インターフェイスでのみ機能し、管理インターフェイス用に設定されたDNSサーバーから情報を返します。データインターフェイスにさまざまなサーバーを設定する場合、データインターフェイスを通過するコマンドで FQDN を使用すると、異なる IP アドレスが返されたり、それらの DNS サーバーが名前を解決できない場合は IP アドレスがまったく返されないことがあります。

例

次に、FQDN www.example.com の IP アドレスを検索する例を示します。このアドレスは、出力の ANSWER セクションで強調表示されます。出力の末尾近くにある SERVER 表示は、解決を返した DNS サーバーの IP アドレスを示しています（この例の IP アドレスはサニタイズされています）。

ヘッダーの NOERROR ステータスは、要求が成功したことを示しています。その他の値はエラーを表します。たとえば、NXDOMAIN は、応答側の DNS サーバーにドメイン名が存在しないことを意味します。Linux の dig コマンドの出力の読み取りの詳細については、インターネットを検索してください。

```
> dig www.example.com
; <<>> DiG 9.11.4 <<>> www.example.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14008
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 88335c9f3dc2ca124e36b5eb60db9067b6cae4de2ea5bffb (good)
```

```
;; QUESTION SECTION:
;www.example.com.               IN      A

;; ANSWER SECTION:
www.example.com.        0       IN      A       93.184.216.34
;; AUTHORITY SECTION:
example.com.            58911   IN      NS      a.iana-servers.net.
example.com.            58911   IN      NS      b.iana-servers.net.

;; ADDITIONAL SECTION:
a.iana-servers.net.     0       IN      A       199.43.135.53

;; Query time: 12 msec
;; SERVER: 10.163.47.11#53(10.163.47.11)
;; WHEN: Tue Jun 29 21:28:07 UTC 2021
;; MSG SIZE  rcvd: 152
```

dir

ディレクトリの内容を表示するには、dir コマンドを使用します。

dir ［**/all**］［**all-filesystems**］［**/recursive**］［ **disk0:** | **disk***n***:** | **flash:** | **system:**］［*path*］［*filename*］

構文の説明

/all	（任意）すべてのファイルを表示します。
/recursive	（任意）ディレクトリの内容を再帰的に表示します。
all-filesystems	（任意）すべてのファイル システムのファイルを表示します。
disk0:	（任意）内部フラッシュメモリを指定し、続けてコロンを入力します。
disk*n***:**	（任意）オプションの外部フラッシュドライブを示します。*n* でドライブ番号を指定します。通常は disk1 です。
flash:	（任意）デフォルト フラッシュ パーティションのディレクトリの内容を表示します。
path	（任意）特定のパスを指定します。
filename	（任意）ファイルの名前を指定します。
system:	（任意）ファイル システムのディレクトリの内容を表示します。

コマンド デフォルト

ディレクトリを指定しない場合、ディレクトリはデフォルトで現在の作業ディレクトリになります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、ディレクトリの内容を表示する例を示します。

```
> dir
Directory of disk0:/
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

Command	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

dns update

DNS ポーリングタイマーの有効期限を待機せずに、指定されたホスト名を解決する DNS ルックアップを開始するには、**dns update** コマンドを使用します。

dns update ［**host** *fqdn_name*］［**timeout seconds** *number*］

構文の説明

host *fqdn_name*	DNS アップデートを実行するホストの完全修飾ドメイン名を指定します。
timeout seconds *number*	ルックアップ動作のタイムアウトを秒単位で指定します（3 ～ 30）。デフォルトは 30 です。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DNS ポーリング タイマーの有効期限を待機しないで、指定されたホスト名を解決する DNS ルックアップをすぐに開始します。ホスト名を指定せずに DNS 更新を実行すると、アクセス制御ルールで使用されるすべての名前（アクティブ化済みと認識される）が解決されます。コマンドの実行が終了すると、システムのコマンドプロンプトに「Done」と表示され、syslog メッセージが生成されます。

例

次の例では、アクセス制御ルールで使用されるすべての FQDN の DNS 更新を実行します。

```
> dns update
INFO: update dns process started
> [Done]
```

関連コマンド

Command	説明
clear dns	FQDN ネットワークオブジェクトの DNS 解決を削除します。
show dns	FQDN ネットワークオブジェクトの DNS 解決を表示します。

eotool コマンド

eotool コマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。

exit

CLI を終了するには、**exit** コマンドを使用します。

exit

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

通常の CLI では、**exit** および **logout** コマンドの動作は同じであり、デバイスとの SSH セッションを閉じます。

エキスパートモードの場合、**exit** を実行するとエキスパートモードが終了し、通常の CLI に戻ります。

診断 CLI（**system support diagnostic-cli**）を使用している場合、**exit** コマンドを実行すると特権 EXEC モードからユーザー EXEC モードに戻ります。

例

次に、**exit** コマンドを使用して CLI への SSH 接続を閉じる例を示します。

```
> exit
```

次に、**exit** コマンドを使用して、診断 CLI の特権 EXEC モード（プロンプトで **#** 記号で表される）からユーザー EXEC モードに戻る例を示します。ログオフメッセージは無視できます。CLI セッションはアクティブなままです。

```
firepower# exit
Logoff
Type help or '?' for a list of available commands.
firepower>
```

関連コマンド

Command	説明
logout	CLI セッションからログオフします。

expert

一部の手順で必要となるエキスパートモードを開始するには、**expert** コマンドを使用します。

expert

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

マニュアルの手順で求められた場合、または Cisco Technical Assistance Center から求められた場合のみ、エキスパートモードを使用します。

注意 エキスパートモードでコマンドを実行しても、結果が Device Manager に反映されない場合があります。意図しない結果を避けるために、エキスパートモードでのみ記載されたコマンド、またはシスコテクニカルサポートから指示されたコマンドを使用してください。

例

次の例は、エキスパートモードを開始および終了する方法を示しています。エキスパートモードのプロンプトには、username@hostname 情報が表示されます。

```
> expert
admin@firepower:~$
admin@firepower:~$ exit
logout
>
```

関連コマンド

Command	説明
exit	エキスパートモードを終了します。

failover active

スタンバイデバイスをアクティブ状態に切り替えるには、**failover active** コマンドを使用します。アクティブデバイスをスタンバイに切り替えるには、このコマンドの **no** 形式を使用します。

failover active
no failover active

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

スタンバイユニットからのフェールオーバー切り替えを開始するには **failover active** コマンドを使用し、アクティブユニットからのフェールオーバー切り替えを開始するには **no failover active** コマンドを使用します。この機能を使用して、障害が発生したユニットを稼働させたり、メンテナンスのためにアクティブ ユニットをオフラインにしたりできます。ステートフル フェールオーバーを使用していない場合、すべてのアクティブ接続がドロップされるため、クライアントはフェールオーバーの発生後、接続を再確立する必要があります。

例

次に、スタンバイユニットをアクティブに切り替える例を示します。

```
> failover active
```

関連コマンド

Command	説明
failover reset	デバイスを障害発生状態からスタンバイに移行します。

failover exec

フェールオーバーペアの特定のユニットでコマンドを実行するには、 **failover exec** コマンドを使用します。

failover exec {**active** | **standby** | **mate**} *cmd_string*

構文の説明

active	コマンドをフェールオーバーペアのアクティブユニットに対して実行することを指定します。
cmd_string	実行するコマンド。サポートされているコマンドについては、CLIのヘルプを参照してください。
mate	コマンドをフェールオーバー ピアに対して実行することを指定します。
standby	コマンドをフェールオーバーペアのスタンバイユニットに対して実行することを指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

failover exec コマンドを使用して、フェールオーバーペアの特定のユニットにコマンドを送信できます。

コマンドの出力は現在の端末セッションに表示されるため、**failover exec** コマンドを使用し、ピア装置で **show** コマンドを発行して、その結果を現在の端末で確認できます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

制限事項

- コマンドの完成およびコンテキストヘルプは、*cmd_string* 引数のコマンドでは使用できません。
- **debug**（**undebug**）コマンドを **failover exec** コマンドと一緒に使用することはできません。
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec mate failover exec mate** コマンドのような、再帰的な **failover exec** コマンドは入力できません。
- ユーザーの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

例

次に、**failover exec** コマンドを使用して、フェールオーバーピアのフェールオーバー設定を表示する例を示します。コマンドはアクティブユニットであるプライマリユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
> failover exec mate show running-config failover
failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
```

次に、**failover exec** コマンドを使用して、**show interface** コマンドをスタンバイユニットに送信する例を示します。

```
> failover exec standby show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
```

```
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
...
```

次に、ピアユニットに対して不正なコマンドを発行したときにエラーメッセージが返され、そのエラー メッセージが表示される例を示します。

```
> failover exec mate bad command
bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

次に、フェールオーバーが無効になっている場合に **failover exec** コマンドを使用すると返されるエラーメッセージの例を示します。

```
> failover exec mate show failover
ERROR: Cannot execute command on mate because failover is disabled
```

関連コマンド

Command	説明
debug fover	フェールオーバー関連のデバッグ メッセージを表示します。
debug xml	**failover exec** コマンドによって使用される XML パーサーのデバッグ メッセージを表示します。
show failover exec	**failover exec** コマンドモードを表示します。

failover reload-standby

スタンバイユニットを強制的にリブートするには、**failover reload-standby** コマンドを使用します。

failover reload-standby

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー ユニットが同期化されないときにこのコマンドを使用します。スタンバイユニットが再起動し、起動終了後にアクティブ ユニットと再同期化されます。

例

次に、アクティブユニットで **failover reload-standby** コマンドを使用して、スタンバイユニットを強制的にリブートする例を示します。

```
> failover reload-standby
```

failover reset

障害が発生したデバイスを障害のない状態に復元するには、**failover reset** コマンドを入力します。

failover reset

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

failover reset コマンドを使用すると、障害が発生したユニットを、障害が発生していない状態にすることができます。**failover reset** コマンドはいずれのユニットでも入力できますが、常にアクティブユニットでコマンドを入力することを推奨します。アクティブユニットで **failover reset** コマンドを入力すると、スタンバイユニットが障害の発生していない状態に復元されます。

show failover コマンドを使用することにより、ユニットのフェールオーバーステータスを表示できます。

例

次に、障害が発生したユニットを障害が発生していない状態に変更する例を示します。

```
> failover reset
```

関連コマンド

Command	説明
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

file copy

FTP 経由で common ディレクトリからリモートホストにファイルを転送するには、**file copy** コマンドを使用します。

file copy *host_name user_id path filename_1* ［*filename_2 ... filename_n*］

構文の説明

host_name	ターゲットリモートホストの名前または IP アドレスを指定します。
user_id	リモートホストのユーザーを指定します。
path	リモートホストの宛先パスを指定します。
filename_1 ～ *filename_n*	common ディレクトリから転送するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。

コマンド デフォルト

このコマンドは、システムがトラブルシューティング ファイルを書き込む common ディレクトリからのみファイルを転送します。

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

例

この例では、common ディレクトリ内のすべてのファイルをユーザー **jdoe** 経由でアクセスするリモートホスト **sentinel** 上の **/pub** ディレクトリに転送します。

```
> file copy sentinel jdoe /pub *
```

関連コマンド

Command	説明
file list	common ディレクトリ内のファイルを一覧表示します。
file delete	common ディレクトリからファイルを削除します。
file secure-copy	SCP 経由で common ディレクトリのファイルを転送します。

file delete

commonディレクトリからファイルを消去するには、**file delete** コマンドを使用します。

file delete *filename_1* [*filename_2* **...** *filename_n*]

構文の説明

filename_1 ～ *filename_n*	commonディレクトリから削除するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。

コマンド デフォルト

このコマンドは、システムがトラブルシューティング ファイルを書き込むcommonディレクトリ内のファイルに対してのみ動作します。

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

例

この例では、単一のファイルを削除します。

```
> file delete 10.83.170.31-43235986-2363-11e6-b278-aff0a43948fe-troubleshoot.tar.gz
```

関連コマンド

Command	説明
file list	common ディレクトリ内のファイルを一覧表示します。
file copy	FTP 経由で common ディレクトリのファイルを転送します。
file secure-copy	SCP 経由で common ディレクトリのファイルを転送します。

file list

common ディレクトリ内のファイルを一覧表示するには、**file list** コマンドを使用します。

file list ［*filename_1 ... filename_n*］

構文の説明

filename_1 ～ *filename_n*	common ディレクトリから一覧表示するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、システムがトラブルシューティング ファイルを書き込むcommonディレクトリ内のファイルのみを一覧表示します。ファイル名を指定しない場合は、common ディレクトリ内のすべてのファイルがリストされます。

例

次に、common ディレクトリの内容を表示する例を示します。

```
> file list
May 26 17:46       137474048 /core_1464284811_rackham-sfr.cisco.com_diskmanager_11.21145
Jun 27 20:36        1464696832 /core_1467059810_rackham-sfr.cisco.com_lina_6.21293
```

関連コマンド

Command	説明
file copy	FTP 経由で common ディレクトリのファイルを転送します。
file delete	common ディレクトリからファイルを削除します。
file secure-copy	SCP 経由で common ディレクトリのファイルを転送します。

file secure-copy

SCP経由でcommonディレクトリからリモートホストにファイルを転送するには、**file secure-copy** コマンドを使用します。

file secure-copy *host_name user_id path filename_1* [*filename_2 ... filename_n*]

構文の説明

host_name	ターゲットリモートホストの名前または IP アドレスを指定します。
user_id	リモートホストのユーザーを指定します。
path	リモートホストの宛先パスを指定します。
filename_1 ～ *filename_n*	common ディレクトリから転送するファイルの名前を指定します。複数のファイル名を指定する場合は、空白で区切る必要があります。この引数では、ワイルドカードがサポートされます。

コマンド デフォルト

このコマンドは、システムがトラブルシューティング ファイルを書き込むcommonディレクトリからのみファイルを転送します。

コマンド履歴

リリース	変更内容
6.0.1	このコマンドが導入されました。

例

この例では、common ディレクトリ内のすべてのファイルをユーザー **jdoe** 経由でアクセスするリモートホスト **101.123.31.1** 上の **/tmp** ディレクトリに転送します。

```
> file secure-copy 101.123.31.1 jdoe /tmp *
```

関連コマンド

Command	説明
file copy	FTP 経由で common ディレクトリのファイルを転送します。
file delete	common ディレクトリからファイルを削除します。
file list	common ディレクトリ内のファイルを一覧表示します。

fsck

ファイルシステムのチェックを実行して破損を修復するには、**fsck** コマンドを使用します。

fsck /noconfirm disk*n***:**

構文の説明

disk*n***:**	フラッシュメモリドライブを指定します。*n* はドライブ番号です。
/noconfirm	コマンドがプロンプトなしで実行されるように指定します。このキーワードは必須です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

fsck コマンドは、ファイルシステムに破損がないかどうかをチェックし、破損があった場合には修復を試みます。より恒久的な手順を試みる前に、このコマンドを使用します。

FSCK ユーティリティで（電源障害や異常なシャットダウンなどによる）ディスクの破損箇所が修復される場合、FSCKxxx.REC という名前のリカバリファイルが作成されます。これらのファイルには、FSCK 実行時に回復されたファイルの一部またはファイル全体が含まれています。まれに、データを回復するためにこれらのファイルを調べる必要がある場合があります。通常、これらのファイルは必要なく、安全に削除できます。

（注） FSCK ユーティリティは起動時に自動的に実行されるため、手動で **fsck** コマンドを入力していない場合でもこれらのリカバリファイルが存在する場合があります。

例

次に、フラッシュ メモリのファイル システムをチェックする例を示します。

```
> fsck /noconfirm disk0:
```

関連コマンド

Command	説明
delete	ユーザーに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
format	ファイルシステムをフォーマットします。

help

特定のコマンドのヘルプ情報を表示するには、**help** コマンドを使用します。

help {*command* | **?**}

構文の説明

?	ヘルプを使用できるすべてのコマンドを表示します。
command	CLI ヘルプを表示するコマンドを指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

help コマンドを使用すると、一部のコマンドのヘルプ情報が表示されます。**help** コマンドの後にコマンド名を入力することによって、個々のコマンドのヘルプを参照できます。コマンド名を指定せずに代わりに **?** を入力すると、ヘルプがあるすべてのコマンドがリストされます。

コマンドの一部を入力した後に ? を入力してヘルプを表示することもできます。これにより、コマンド文字列内のその場所で有効なパラメータが表示されます。

例

次に、**traceroute** コマンドのヘルプを表示する例を示します。

```
> help traceroute
USAGE:
        traceroute <destination> [source <src_address|src_intf>]
                   [numeric] [timeout <time>] [ttl <min-ttl> <max-ttl>]
                   [probe <probes>] [port <port-value>] [use-icmp]
DESCRIPTION:
traceroute      Print the route packets take to a network host
SYNTAX:
destination     Address or hostname of destination
src_address     Source address used in the outgoing probe packets
src_intf        Interface through which the destination is accessible
numeric         Do not resolve addresses to hostnames
time            The time in seconds to wait for a response to a probe
min-ttl         Minimum time-to-live value used in probe packets
max-ttl         Maximum time-to-live value used in probe packets
probes          The number of probes to send for each TTL value
port-value      Base UDP destination port used in probes
use-icmp        Use ICMP probes instead of UDP probes
```

history

現在のセッションのコマンドライン履歴を表示するには、**history** コマンドを使用します。

history *limit*

構文の説明

limit	エントリ数の履歴リストのサイズ。サイズを無制限に設定するには、つまり履歴全体を表示するには、「0」を入力します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

上矢印を使用して、過去のコマンドをスクロールすることもできます。

履歴ビューには、コマンドが入力された順序のシーケンス番号が含まれます。

例

このコマンドの出力例を次に示します。

```
> history 0
   48  show environment
   49  show network-static-routes
   50  show network
   51  show running-config
   52  show service-policy
   53  show ntp
   54  show cpu
   55  show memory
   56  history 0
>
```

logging savelog

ログバッファをフラッシュメモリに保存するには、**logging savelog** コマンドを使用します。

logging savelog ［*savefile*］

構文の説明

savefile	（オプション）保存されたログのファイル名。ファイル名を指定しない場合は、次に示すように、ログファイルはデフォルトのタイムスタンプフォーマットを使用して保存されます。 `LOG-YYYY-MM-DD-HHMMSS.TXT` *YYYY* は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存する前に、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに保存されません。ただし、設定されたロギングバッファサイズが 2MB を超える場合、内部ログバッファはフラッシュメモリに書き込まれません。Management Center（リモート）または Device Manager （ローカル）を使用してバッファロギングを設定します。

（注） **logging savelog** コマンドによってバッファはクリアされません。バッファをクリアするには、**clear logging buffer** コマンドを使用します。

例

次に、latest-logfile.txt というファイル名で、ログバッファをフラッシュメモリに保存する例を示します。

```
> logging savelog latest-logfile.txt
>
```

関連コマンド

Command	説明
clear logging buffer	ログバッファが保持している syslog メッセージをすべて消去します。

Command	説明
copy	TFTP サーバーまたは FTP サーバーを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。

logout

CLI を終了するには、**logout** コマンドを使用します。

logout

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

logout コマンドを使用すると、デバイスからログアウトして CLI セッションを終了できます。**exit** コマンドを使用することもできます。

例

次に、デバイスからログアウトする方法の例を示します。

```
> logout
```

memory caller-address

コールトレースまたは発信元 PC 用にプログラムメモリの特定の範囲を設定して、メモリの問題を容易に特定できるようにするには、**memory caller-address** コマンドを使用します。発信元 PC は、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレス範囲を削除するには、このコマンドの no 形式を使用します。

memory caller-address *startPC endPC*
no memory caller-address

構文の説明

endPC	メモリ ブロックの終了アドレス範囲を指定します。
startPC	メモリ ブロックの開始アドレス範囲を指定します。

コマンド デフォルト

メモリを追跡できるように、実際の発信元 PC が記録されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

メモリの問題を特定のメモリブロックに限定するには、**memory caller-address** コマンドを使用します。

場合によっては、メモリ割り当てプリミティブの実際の発信元 PC が、プログラムの多くの場所で使用されている既知のライブラリ関数であることがあります。プログラムの個々の場所を特定するには、そのライブラリ関数の開始プログラム アドレスおよび終了プログラム アドレスを設定し、それによってライブラリ関数の呼び出し元のプログラムアドレスを記録します。

（注） 発信元アドレスの追跡を有効にすると、デバイスのパフォーマンスが一時的に低下することがあります。

例

次に、**memory caller-address** コマンドで設定したアドレスの範囲、および **show memory caller-address** コマンドによる表示結果の例を示します。

```
> memory caller-address 0x00109d5c 0x00109e08
> memory caller-address 0x009b0ef0 0x009b0f14
> memory caller-address 0x00cf211c 0x00cf4464
> show memory caller-address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

関連コマンド

Command	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory	物理メモリの最大量とオペレーティング 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 memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory profile	デバイスのメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory caller-address	デバイスに設定されているアドレスの範囲を表示します。

memory delayed-free-poisoner

memory delayed-free-poisoner コマンドを使用して、delayed free-memory poisoner ツールのパラメータを設定します。delayed free-memory poisoner ツールを有効にするには、**memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールを無効にするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションによってメモリが解放された後、解放メモリの変化をモニターできます。

memory delayed-free-poisoner {**enable** | **desired-fragment-count** *frag_count* | **desired-fragment-size** *frag-size* | **threshold** *heap_use_percent* | **validate** | **watchdog-percent** *watchdog_limit*}
no memory delayed-free-poisoner enable

構文の説明

enable	delayed free-memory poisoner ツールの操作を開始します。
desired-fragment-count *frag_count*	poisonerのキューに保持するメモリフラグメントの数を設定します。有効な値の範囲は 0 ー 8192 です。デフォルトは 16 です。
desired-fragment-size *frag-size*	poisoner のキューに保持する連続した空きメモリフラグメントのサイズをバイト単位で設定します。有効な値の範囲は 0 ー 268435456 です。デフォルトは 102400 です。
threshold *heap_use_percent*	poisoner のキューからメモリが解放されるシステムメモリ使用率のパーセンテージしきい値を 0 ー 100 の範囲で設定します。デフォルトは 100 です。
validate	delayed free-memory poisoner キュー内の全要素の検証を強制実行します。
watchdog-percent *watchdog_limit*	ウォッチドッグ制限をウォッチドッグしきい値（15秒）のパーセンテージとして設定します。値の範囲は 10 ～ 100 です。デフォルトは 50 です。

コマンド デフォルト

memory delayed-free-poisoner enable コマンドはデフォルトでは無効になっています。

デフォルトの **desired-fragment-count** は 16 です。

デフォルトの **desire-fragment-size** は 102400 です。

デフォルトの **watchdog-percent** は 50 です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに大きな影響を及ぼします。このコマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。システムの使用率が高い間は、実働環境では実行しないでください。

このツールを有効にすると、デバイスで実行されているアプリケーションによるメモリ解放要求が FIFO キューに書き込まれます。要求が poisoner のキューに書き込まれるたびに、それに伴うメモリバイトのうち、下位メモリ管理には必要ないバイトが、値 0xcc で書き込まれて「改ざん」されます。

メモリ解放要求は、システムの空きメモリプールにある量よりも多くのメモリがアプリケーションで必要になるまで、キューに残ります。より多くのメモリが必要になると、poisoner はキュー内の少なくとも **desired-fragment-count** メモリバッファの **desired-fragment-size** バイトをシークし、そのメモリをキューからプルして検証します。**desired-fragment-size** と **desired-fragment-count** の値を変更することで、poisoner が大量のメモリ要求を処理するのにかかる時間を調整できます。

メモリに変更がない場合、メモリはシステムの空きメモリプールに返され、poisoner は最初に要求を行ったアプリケーションからのメモリ要求を再発行します。このプロセスは、要求元のアプリケーションに対して十分なメモリが解放されるまで繰り返されます。

改ざんされたメモリに変更があった場合、システムは強制的にクラッシュし、クラッシュの原因を確認するために使用できる診断出力を生成します。

delayed free poisoner には、プロセスの過剰なリソース使用を防ぐためのウォッチドッグメカニズムが含まれています。ウォッチドッグしきい値は 15 秒で、その間 CPU を放棄せずにプロセスが継続的に実行されると、poisoner はシステムを強制的にクラッシュさせます。

ウォッチドッグの動作は、ウォッチドッグ制限を設定することで調整できます。ウォッチドッグ制限は 15 秒のウォッチドッグしきい値の割合を示します。デフォルトは 50% です。したがって、delayed free poisoner がアクティブな場合、デフォルトでは、プロセスが CPU を放棄せずに 7.5 秒間連続して実行されると、そのプロセスからの追加のメモリ割り当て要求は、プロセスが再スケジュールされるまで失敗します。この動作は、ウォッチドッグ制限の値を変更することで調整できます。

過剰なメモリフラグメンテーションを防止し、システム CPU の負荷を軽減するために、poisoner がメモリをキューからシステムメモリプールに自動的に解放する空きメモリ使用率のパーセンテージ **threshold** を設定できます。（デフォルトでは、poisoner はシステムメモリが使い果たされるまでメモリをキューから解放しません）。

delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。**memory delayed-free-poisoner validate** コマンドを使用して手動で検証を開始することもできます。要素に予期しない値が含まれている場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。予期しない値が存在しない場合、要素はキューに残り、ツールによって正常に処理されます。**memory delayed-free-poisoner validate** コマンドを実行しても、キュー内のメモリはシステムメモリプールに返されません。

このコマンドの **no** 形式を実行すると、キュー内の要求で参照されるすべてのメモリが検証されずに空きメモリプールに返され、すべての統計カウンタがクリアされます。

例

次に、delayed free-memory poisoner ツールをイネーブルにする例を示します。

```
> memory delayed-free-poisoner enable
```

次に、delayed free-memory poisoner ツールが不正なメモリ再利用を検出した場合の出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

次の表では、出力の重要な部分について説明されています。

表 *1:* 不正なメモリ使用に関する出力の説明

フィールド	説明
heap region	要求元のアプリケーションが使用できるメモリ領域のアドレス領域およびサイズ。これは、要求されたサイズと同じ値ではなく、メモリ要求が行われたときにシステムがメモリを配分できるように小さくなることがあります。
memory address	障害が検出されたメモリの位置。
byte offset	バイトオフセットはヒープ領域の先頭を基準にしており、このアドレスから始まるデータ構造を保持するためにフィールドが変更された場合には、バイトオフセットを使用してそのフィールドを見つけることができます。値が0か、またはヒープ領域バイトカウントよりも大きい値である場合は、問題が下位ヒープパッケージの予期しない値であることを示している可能性があります。
allocated by/freed by	この特定のメモリ領域に関して実施された最後の malloc/calloc/realloc および解放要求の命令アドレス。

フィールド	説明
Dumping...	検出された障害がヒープ メモリ領域の先頭にどれだけ近いかに応じて、1 つまたは 2 つのメモリ領域のダンプ。システム ヒープ ヘッダーに続く 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュとキュー リンクを保持するために使用するメモリです。システム ヒープ トレーラが検出されるまでの領域内のそれ以外のバイトは、0xcc に設定する必要があります。

関連コマンド

Command	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory logging

メモリロギングを有効にするには、**memory logging** コマンドを使用します。メモリロギングを無効にするには、このコマンドの **no** 形式を使用します。

memory logging 1024-4194304 ［**wrap** ［**size** ［**1-2147483647**］ | **process** *process-name* ］
no memory logging

構文の説明

1024-4194304	メモリ ロギング バッファのロギング エントリの数を指定します。指定する必要がある引数はこれだけです。
process *process-name*	モニター対象のプロセスを指定します。 （注） Checkheaps プロセスは、非標準の方法でメモリ アロケータを使用するため、プロセスとして完全に無視されます。
size 1-2147483647	モニターするサイズおよびエントリ数を指定します。
wrap	バッファのラップ時にバッファを保存します。保存できるのは一度だけです。複数回ラップされると上書きされる可能性があります。バッファがラップすると、そのデータの保存をイネーブルにするトリガーがイベント マネージャに送信されます。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

メモリ ロギング パラメータを変更するには、それをディセーブルにしてから、再度イネーブルにします。**show memory logging** コマンドを使用してログを表示します。

例

次に、メモリ ロギングをイネーブルにする例を示します。

```
> memory logging 202980
```

関連コマンド

Command	説明
show memory logging	メモリ ロギングの結果を表示します。

memory profile enable

メモリ使用状況（メモリプロファイリング）のモニタリングを有効にするには、**memory profile enable** コマンドを使用します。メモリプロファイルリングを無効にするには、このコマンドの **no** 形式を使用します。

memory profile enable ［**peak** *peak_value*］
no memory profile enable ［**peak** *peak_value*］

構文の説明

peak *peak_value*	メモリ使用状況のスナップショットを使用率ピーク バッファに保存するメモリ使用状況しきい値を指定します。このバッファの内容を後で分析して、システムのピーク時のメモリ ニーズを判断できます。

コマンド デフォルト

デフォルトでは、メモリ プロファイリングはディセーブルになっています。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

メモリプロファイリングを有効にする前に、**memory profile text** コマンドを使用して、プロファイリングするメモリのテキスト範囲を設定する必要があります。

clear memory profile コマンドを入力するまで、一部のメモリはプロファイリングシステムによって保持されます。**show memory profile status** コマンドの出力を参照してください。

（注） メモリプロファイリングをイネーブルにすると、デバイスのパフォーマンスが一時的に低下する場合があります。

例

次に、メモリ プロファイリングをイネーブルにする例を示します。

```
> memory profile enable
```

関連コマンド

Command	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	デバイスのメモリ使用状況（プロファイリング）に関する情報を表示します。

memory profile text

プロファイリングするメモリのプログラムテキスト範囲を設定するには、**memory profile text** コマンドを使用します。無効にするには、このコマンドの no 形式を使用します。

memory profile text {*startPC endPC* | **all**} *resolution*
no memory profile text {*startPC endPC* | **all**} *resolution*

構文の説明

all	メモリ ブロックのテキスト範囲全体を指定します。
endPC	メモリ ブロックの終了テキスト範囲を指定します。
resolution	ソーステキスト領域のトレースの精度を 1 ー 44582263 の範囲で設定する必要があります。
startPC	メモリ ブロックの開始テキスト範囲を指定します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

テキスト範囲が小さい場合、精度を「4」にすると、命令への呼び出しが正常に追跡されます。テキスト範囲が大きい場合、精度を粗くしても初回通過には十分であり、範囲は次回の通過でさらに小さな領域にまで絞り込むことができます。

メモリプロファイリングを開始するには、**memory profile text** コマンドでテキスト範囲を入力した後、続けて **memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリプロファイリングはディセーブルになっています。

（注） メモリプロファイリングをイネーブルにすると、デバイスのパフォーマンスが一時的に低下する場合があります。

例

次に、精度を 100 にして、プロファイリングするメモリのテキスト範囲を設定する例を示します。

```
> memory profile text all 100
```

次に、メモリ プロファイリングのテキスト範囲のコンフィギュレーションおよびステータス（OFF）を表示する例を示します。

```
> show memory profile status
```

```
InUse profiling: OFF
Peak profiling: OFF
Memory used by profile buffers: 0 bytes
Profile:
0x00007efc3e0227a8-0x00007efc40aa1f8e(00000100)
```

（注） メモリプロファイリングを開始するには、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリ プロファイリングはディセーブルになっています。

関連コマンド

Command	説明
clear memory profile	メモリ プロファイリング機能によって保持されているバッファをクリアします。
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
show memory profile	デバイスのメモリ使用状況（プロファイリング）に関する情報を表示します。

memory tracking

ヒープメモリ要求の追跡を有効にするには、**memory tracking** コマンドを使用します。メモリ追跡を無効にするには、このコマンドの **no** 形式を使用します。

memory tracking {**enable** | **allocates-by-threshold** *min_allocates* | **bytes-threshold** *min_bytes* | **filter-from-address-pool** *address*}
no memory tracking enable

構文の説明

enable	メモリの追跡を有効にします。
allocates-by-threshold *min_allocates*	発信者のアドレスプールのエントリには、少なくともこの数の割り当てコールを含める必要があります（0 ー 4294967295）。
bytes-threshold *min_bytes*	発信者のアドレスプールのエントリは、少なくともこのバイト数のメモリを消費する必要があります（0 ー 4294967295）。
filter-from-address-pool *address*	このアドレスのアドレスプールのエントリを除外します。アドレスを決定するには、最初にトラッキングを有効にしてから、show memory tracking address を使用します。「memory tracking address pool」リストで「allocated by」アドレスを探します。たとえば、次のように表示されます。 ...allocated by 0x00007efc3f80e508 次を使用して除外できます。 **filter-from-address-pool 0x00007efc3f80e508**

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

次に、ヒープ メモリ要求の追跡をイネーブルにする例を示します。

```
> memory tracking enable
```

関連コマンド

Command	説明
clear memory tracking	現在収集されているすべての情報をクリアします。
show memory tracking	メモリトラッキングの結果を表示します。

more

ファイルの内容を表示するには、**more** コマンドを使用します。

more [**/ascii** | **/binary** | **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **tftp:**] *filename*

構文の説明

/ascii	（任意）バイナリ ファイルをバイナリ モード、ASCII ファイルをバイナリ モードで表示します。
/binary	（任意）任意のファイルをバイナリ モードで表示します。
/ebcdic	（任意）バイナリ ファイルを EBCDIC で表示します。
disk0:	（任意）内部フラッシュメモリ上のファイルを表示します。
disk1:	（任意）外部フラッシュメモリカード上のファイルを表示します。
filename	表示するファイルの名前を指定します。
flash:	（任意）内部フラッシュメモリを指定し、続けてコロンを入力します。ASA 5500 シリーズの適応型セキュリティアプライアンスでは、**flash** キーワードは **disk0** のエイリアスです。
ftp:	（任意）FTP サーバー上のファイルを表示します。
http:	（任意）Web サイト上のファイルを表示します。
https:	（任意）セキュアな Web サイト上のファイルを表示します。
tftp:	（任意）TFTP サーバー上のファイルを表示します。

コマンド デフォルト

ASCII モード。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

system support view-files コマンドは、ログファイルを検索および表示するための優れたオプションです。

例

次に、「test.cfg」というローカル ファイルの内容を表示する例を示します。

```
> more test.cfg
: Saved
```

```
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

関連コマンド

Command	説明
cd	指定されたディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。

Command	説明
system support view-files	ログファイルの内容を検索して表示します。

nslookup（非推奨）

完全修飾ドメイン名の IP アドレスを検索する、または IP アドレスの完全修飾ドメイン名を検索するには、**nslookup** コマンドを使用します。

nslookup {*hostname* | *ip_address*}

構文の説明

hostname	IP アドレスを検索するホストの完全修飾ドメイン名。たとえば、www.example.com などです。
ip_address	完全修飾ドメイン名を検索するホストの IP アドレス。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	このコマンドは機能しなくなり、廃止されました。
7.1	このコマンドが削除され、**dig** コマンドに置き換えられました。

使用上のガイドライン

完全修飾ドメイン名を許可するコマンドの中には、管理インターフェイス用に設定された DNS サーバーを使用して完全修飾ドメイン名から IP アドレスを検索できないものがあります。データインターフェイスを通過するコマンド用に DNS サーバーが設定されていない場合は、**nslookup** コマンドを使用して IP アドレスを特定し、そのコマンドで IP アドレスを使用します。

nslookup コマンドは、特定の IP アドレスの完全修飾ドメイン名を判断する場合にも役立ちます。

例

次に、www.cisco.com の IP アドレスを検索する例を示します。最初の [Server] および [Address] 情報には、DNS サーバー（完全修飾ドメイン名の場合もあります）、IP アドレス、およびポートが表示されます（この例では偽のアドレスを使用しています）。その後の情報は、入力した名前の正規の（実際の）ホスト名と IP アドレスを示します。

```
> nslookup www.cisco.com
Server:         10.102.6.247
Address:        10.102.6.247#53

www.cisco.com   canonical name = origin-www.cisco.com.
Name:   origin-www.cisco.com
Address: 173.37.145.84
```

次の例は、逆引き参照を実行し、IP アドレスのホスト名を決定する方法を示しています。最初の情報は、使用されている DNS サーバーに関するものです。マッピングされたホスト名が **name =** フィールドに示されます。

```
> nslookup 173.37.145.84
Server:         10.102.6.247
Address:        10.102.6.247#53

84.145.37.173.in-addr.arpa      name = www2.cisco.com.
```

packet-tracer

ファイアウォールルールをテストする5つのタプルを指定して、トラブルシューティング用にパケットトレーシングを有効にするには、**packet-tracer** コマンドを使用します。ここでは、わかりやすいように、ICMP、TCP、および IP の各パケットのモデリング別に構文を示します。複数のパケットを再生し、 **pcap** キーワードを使用して完全なワークフローをトレースできます。

packet-tracer input *ifc_name* **icmp** {*sip* | **user** *username*} *type code* [*ident*] {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
packet-tracer input *ifc_name* {**tcp** | **udp**} {*sip* | **user** *username*} *sport* {*dip* | **fqdn** *fqdn-string*} *dport* [**detailed**] [**xml**]
packet-tracer input *ifc_name* **rawip** {*sip* | **user** *username*} *protocol* {*dip* | **fqdn** *fqdn-string*} [**detailed**] [**xml**]
packet-tracer input *ifc_name* **pcap** *pcap_filename* [**bypass-checks** | **decrypted** | **detailed** | **persist** | **transmit** | **xml** | **json** | **force**]

構文の説明

bypass-checks	（任意）シミュレートされたパケットのセキュリティチェックをバイパスします。
decrypted	（任意）シミュレートされたパケットを、復号された IPSec/SSL VPN と見なします。
code	ICMP パケット トレースの ICMP コードを指定します。
detailed	（オプション）トレース結果の詳細な情報を表示します。
dip	パケット トレースの宛先アドレス（IPv4 または IPv6）を指定します。
dport	TCP/UDP/SCTP パケット トレースの宛先ポートを指定します。
fqdn *fqdn-string*	ホストの完全修飾ドメイン名を指定します。IPv4 の FQDN のみがサポートされます。
force	既存の pcap トレースを削除し、新しい pcap ファイルを実行します。
icmp	使用するプロトコルとして ICMP を指定します。
ident	（任意）ICMP パケット トレースの ICMP ID を指定します。
inline-tag *tag*	レイヤ 2 CMD ヘッダーに埋め込まれているセキュリティ グループ タグの値を指定します。有効な値の範囲は 0 ～ 65533 です。
input *ifc_name*	パケットをトレースする送信元インターフェイス名を指定します。
json	（任意）トレース結果を JSON 形式で表示します。
pcap	pcap を入力として指定します。

pcap_filename	トレース用のパケットを含む pcap ファイル名。
protocol	raw IP パケット トレーシングのプロトコル番号（0 ～ 255）を指定します。
persist	（任意）長期間のトレースを有効にし、クラスタでのトレースも有効にします。
rawip	使用するプロトコルとして raw IP を指定します。
sip	パケット トレースの送信元アドレス（IPv4 または IPv6）を指定します。
sport	TCP/UDP/SCTP パケット トレースの送信元ポートを指定します。
tcp	使用するプロトコルとして TCP を指定します。
transmit	（任意）シミュレートされたパケットがデバイスから送信できるようにします。
type	ICMP パケット トレースの ICMP タイプを指定します。
udp	使用するプロトコルとして UDP を指定します。
user *username*	送信元 IP アドレスとしてユーザーを指定する場合に domain\user の形式でユーザー アイデンティティを指定します。ユーザーに対して最後にマッピングされたアドレス（複数ある場合）がトレースに使用されます。
xml	（オプション）トレース結果を XML 形式で表示します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	出力が強化され、パケットのルーティング中にパケットを許可/拒否する特定の理由を提供するようになりました。
7.1	トレースの入力として pcap ファイルを使用できるように、packet-tracer コマンドが拡張されました。

使用上のガイドライン

パケットのキャプチャに加えて、脅威に対する防御デバイスを介してパケットの寿命をトレースして、想定どおりに動作しているかどうかを確認できます。**packet-tracer** コマンドを使用すると、次の操作を実行できます。

- 実働ネットワークにおけるすべてのパケット ドロップをデバッグします。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。

- パケットに適用可能なすべてのルール、およびルールが追加される原因となったCLI行を表示する。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスにトレーサ パケットを挿入する。

packet-tracer コマンドは、パケットに関する詳細情報と、脅威に対する防御 デバイスによるパケットの処理方法を表示します。コンフィギュレーションからのコマンドが原因でパケットがドロップしたのではない場合、**packet-tracer** コマンドにより、原因に関する詳細な情報が読みやすい形式で表示されます。たとえば、ヘッダーの検証が無効なためパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」メッセージが表示されます。

packet-tracer が単一のパケットを注入してトレースしている間、**pcap** キーワードにより、パケットトレーサは複数のパケット（最大100パケット）を再生し、フロー全体をトレースできます。pcap ファイルを入力として提供し、さらに分析するために XML または JSON 形式で結果を取得できます。トレース出力をクリアするには、**clear packet-tracer** の **pcap trace** サブコマンドを使用します。トレースの進行中は、トレース出力を使用できません。

例

次に、入力として pcap ファイルを使用してパケットトレーサを実行する例を示します。

```
> packet-tracer input inside pcap http_get.pcap detailed xml
```

次に、既存の pcap トレースバッファをクリアし、入力として pcap ファイルを提供することにより、パケットトレーサを実行する例を示します。

```
> packet-tracer input inside pcap http_get.pcap force
```

次に、HTTP ポート 10.100.10.10 から 10.100.11.11 への TCP パケットをトレースする例を示します。暗黙の拒否アクセス ルールによってパケットがドロップされることを示す結果が表示されます。

```
> packet-tracer input outside tcp 10.100.10.10 80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
```

```
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

次の例では、ネクストホップのARPエントリが含まれる直接接続されたホストでTCPパケットを追跡します。

```
firepower(config)# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102
 80 detailed
Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any
```

```
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
```

```
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

次の例では、ネクストホップに対する有効なARPエントリがないためにドロップされたTCPパケットを追跡します。ドロップされた理由では、ARPテーブルをチェックするためのヒントも提供されています。

```
<Displays same phases as in the previous example till Phase 8>

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has
entry for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

次の例では、NAT と到達可能なネクストホップを使用した準最適ルーティングのパケットトレーサを示しています。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
firepower(config)# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80
detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
```

```
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
```

```
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
```

```
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

次の例では、NAT を使用した準最適ルーティングのパケットトレーサを示しています。ここでは、到達不能なネクストホップが原因でパケットがドロップされます。

```
firepower(config)# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

firepower(config)# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

関連コマンド

Command	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
show packet-tracer	PCAP ファイルに対して最後に実行されたパケットトレーサのトレースバッファ出力を表示します。

perfmon

コンソールにパフォーマンス情報を表示するには、**perfmon** コマンドを使用します。

perfmon {**verbose** | **interval***seconds* | **settings**}

構文の説明

verbose	パフォーマンスモニター情報をコンソールに表示します。デフォルトでは、perfmon settings で「quiet」と表示される情報は表示されません。 診断 CLI で **perfmon verbose** をオフにする必要があります。
interval *seconds*	コンソールでパフォーマンス表示がリフレッシュされるまでの秒数を指定します。
settings	間隔、および perfmon が quiet と verbose のどちらであるかを表示します。

コマンド デフォルト

デフォルトの間隔は、120 秒です。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

perfmon コマンドを使用すると、デバイスのパフォーマンスをモニターできます。**show perfmon** コマンドを使用すると、情報がすぐに表示されます。

perfmon verbose コマンドを使用すると、間隔ごとにコンソールに情報が表示されます。

情報は、コンソールポートで CLI に実際に接続している場合、または診断 CLI（**system support diagnostic-cli**）を使用している場合のみ自動的に表示されます。別のポートで CLI（管理インターフェイスを含む）を使用している場合は、**show console-output** コマンドを使用して自動的に生成された情報を表示します。または、このコマンドを使用せず、**show perfmon** コマンドを直接使用します。

このコマンドは、診断 CLI でのみ使用することを推奨します。

（注） 通常の CLI から **verbose** をオフにすることはできません。代わりに、診断 CLI で特権 EXEC モードからオフにする必要があります。「例」の項を参照してください。

例

次に、パフォーマンスモニター統計情報を 120 秒間隔でコンソールに表示する例を示します。出力の「Fixup」統計情報は、関連するプロトコル検査エンジンを指しています。

```
> perfmon verbose
> perfmon settings
interval: 120 (seconds)
verbose
> show console-output
...
Message #109 :
Message #110 : PERFMON STATS:                      Current      Average
Message #111 : Xlates                                0/s          0/s
Message #112 : Connections                           0/s          0/s
Message #113 : TCP Conns                             0/s          0/s
Message #114 : UDP Conns                             0/s          0/s
Message #115 : URL Access                            0/s          0/s
Message #116 : URL Server Req                        0/s          0/s
Message #117 : TCP Fixup                             0/s          0/s
Message #118 : TCP Intercept Established Conns       0/s          0/s
Message #119 : TCP Intercept Attempts                0/s          0/s
Message #120 : TCP Embryonic Conns Timeout           0/s          0/s
Message #121 : FTP Fixup                             0/s          0/s
Message #122 : AAA Authen                            0/s          0/s
Message #123 : AAA Author                            0/s          0/s
Message #124 : AAA Account                           0/s          0/s
Message #125 : HTTP Fixup                            0/s          0/s
Message #126 :
...
```

次に、冗長モードをオフにする例を示します。これは、診断 CLI から行う必要があります。

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower> enable
Password: <Press return, do not enter a password>

firepower# perfmon quiet
firepower# perfmon settings
interval: 120 (seconds)
quiet
firepower# <Press Ctrl+a, d>

Console connection detached.
> perfmon settings
interval: 120 (seconds)
quiet
```

関連コマンド

Command	説明
show perfmon	パフォーマンス情報を表示します。

pigtail コマンド

pigtail コマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。

書き込まれたログを表示する場合は、**pigtail** の代わりに **tail-logs** コマンドを使用します。

⚠

注意 ディスク使用率が高くなる可能性があるため、pigtail プロセスを実行中のままにしないでください。このプロセスがポリシーの展開中に実行されていると、展開の妨げになる可能性があります。pigtail プロセスを停止する方法については、Cisco Technical Assistance Center にお問い合わせください。

ping

指定したインターフェイスから IP アドレスへの接続をテストするには、**ping** コマンドを使用します。使用できるパラメータは、通常の ICMP ベースの ping、TCP の ping、および「システム」の ping とで異なります。また、システムの ping は管理インターフェイスから実行されますが、他のタイプの ping はデータインターフェイスを通過します。テストでは、必ず正しいタイプの ping を使用してください。

ping ［**interface** *if_name* | **vrf** *name*］ *host* ［**repeat** *count*］ ［**timeout** *seconds*］ ［**data** *pattern*］ ［**size** *bytes*］ ［**validate**］
ping tcp ［**interface** *if_name* | **vrf** *name*］ *host port* ［**repeat** *count*］ ［**timeout** *seconds*］ ［**source** *host port*］
ping system *host*

構文の説明

data *pattern*	（オプション、ICMP のみ）16 ビットデータ パターン（16 進数形式、0 ～ FFFF）を指定します。デフォルトは 0xabcd です。
host	ping の送信先ホストの IPv4 アドレスまたは名前を指定します。ICMP ping の場合は、IPv6 アドレスも指定できます。IPv6 は、TCP またはシステム ping ではサポートされていません。 ping が www.example.com などの完全修飾ドメイン名を使用できるかどうかは、名前を解決する DNS サーバーの可用性に依存します。システム ping は管理インターフェイスに DNS サーバーを使用しますが、他のタイプの ping は管理 DNS サーバーを使用しません。 システム以外のホスト名の ping が機能するには、データインターフェイスの DNS を設定する必要があります。 **ping** がホスト名を解決できない場合、**nslookup** を使用して名前に関連付けられた IP アドレスを特定し、IP アドレスで ping を実行します。
interface *if_name*	（オプション）ICMP の場合、これはホストがアクセス可能なインターフェイス名です。指定しない場合、host は IP アドレスに解決され、宛先インターフェイスを決定するためにルーティング テーブルが参照されます。TCP の場合は、送信元からの SYN パケットの送信に使用する入力インターフェイスを指定します。 Virtual Routing and Forwarding（VRF）が有効なときに **interface** キーワードを指定すると、ping は指定されたインターフェイスの仮想ルーティングテーブルを使用します。
port	（TCP のみ）ping を送信するホストの TCP ポート番号（1 ～ 65535）を指定します。
repeat *count*	（任意）ping 要求を繰り返す回数を指定します。デフォルトは 5 分です。

size *bytes*	（オプション、ICMP のみ）データグラム サイズ（バイト単位）を指定します。デフォルトは 100 です。
source *host port*	（オプション、TCP のみ）ping の送信元の特定の IP アドレスおよびポートを指定します（特定のポートを指定しない場合は port = 0 を使用します）。
system	管理インターフェイスを通じてホストに ping を実行します。データインターフェイスを介した ping とは違い、システム ping のデフォルト数はありません。ping は Ctrl+c を使用して停止するまで続けられます。
tcp	（オプション）TCP での接続をテストします（デフォルトは ICMP です）。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。TCP ping は同時に複数実行することもできます。
timeout *seconds*	（オプション）タイムアウト間隔（秒数）を指定します。デフォルト値は 2 秒です。
validate	（オプション、ICMP のみ）応答データを検証します。
vrf *name*	（任意）Virtual Routing and Forwarding（VRF）（仮想ルータとも呼ばれる）を有効にすると、仮想ルータの名前を指定して、使用する仮想ルーティングテーブルを選択できます。このキーワードは、**interface** キーワードと同時に使用することはできません。 Virtual Routing and Forwarding（VRF）が有効なときに **interface** キーワードを指定すると、ping は指定されたインターフェイスの仮想ルーティングテーブルを使用します。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。
6.6	**vrf** キーワードが追加されました。

使用上のガイドライン

ping コマンドを使用すると、デバイスが接続可能かどうか、またはホストがネットワークで使用可能かどうかを判断できます。

通常の ICMP ベースの ping を使用する場合、それらのパケットの送信を禁止する ICMP ルールがないことを確認してください（ICMP ルールを使用していなければ、すべての ICMP トラフィックが許可されます）。

TCP ping を使用する場合は、指定したポートでの TCP トラフィックの送受信がアクセス ポリシーで許可されている必要があります。

このコンフィギュレーションは、**ping** コマンドで生成されたメッセージに対して、デバイスが応答したり受け入れたりするために必要です。**ping** コマンドの出力は、応答が受け入れられた

かどうかを示します。ホストが応答しない場合は、**ping** コマンドを入力すると、次のようなメッセージが表示されます。

```
> ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

デバイスがネットワークに接続していて、トラフィックを送受信していることを確認するには、**show interface** コマンドを使用します。指定されたインターフェイスの名前は、ping の送信元アドレスとして使用されます。

例

次に、データインターフェイスを介してIPアドレスにアクセスできるかどうかを判断する例を示します。インターフェイスが指定されていないため、アドレスへの到達方法を判断するためにルーティングテーブルが使用されます。

```
> ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次の例では、TCP ping を使用して、データインターフェイスを介してホストにアクセス可能かどうかを判断します。

```
> ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

> ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
```

次の例では、システム ping を実行して、管理インターフェイスから www.cisco.com にアクセスできるかどうかを判断します。ping を停止するには、Ctrl+c を使用する必要があります（出力では ^C で示されます）。

```
> ping system www.cisco.com
PING origin-www.cisco.COM (72.163.4.161) 56(84) bytes of data.
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=1 ttl=242 time=10.6 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=2 ttl=242 time=8.13 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=3 ttl=242 time=8.51 ms
64 bytes from www1.cisco.com (72.163.4.161): icmp_seq=4 ttl=242 time=8.40 ms
^C
--- origin-www.cisco.COM ping statistics ---
```

```
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 8.139/8.927/10.650/1.003 ms
>
```

次の例では、redという名前の仮想ルータのルーティングテーブルを使用して、アドレスに ping を実行します。

```
> ping vrf red 2002::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms
```

関連コマンド

Command	説明
nslookup	ホスト名または IP アドレスの DNS ルックアップを実行します。
show interface	インターフェイス コンフィギュレーションに関する情報を表示します。

pmtool コマンド

pmtool コマンドは、Cisco Technical Assistance Center の指示の下でのみ使用してください。

reboot

デバイスをリブートするには、**reboot** コマンドを使用します。

reboot

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

例

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes

Broadcast message from root@firepower

The system is going down for reboot NOW!
...
```

redundant-interface

アクティブにする冗長インターフェイスのメンバーインターフェイスを設定するには、**redundant-interface** コマンドを使用します。

redundant-interface redundant *number* **active-member** *physical_interface*

構文の説明

active-member *physical_interface*	アクティブ メンバーを設定します。使用可能な物理インターフェイス名（GigabitEthernet0/0 など）を表示するには、show interface コマンドを使用します。両方のメンバー インターフェイスが同じ物理タイプである必要があります。
redundant *number*	冗長インターフェイス ID（**redundant 1** など）を指定します。番号は 1 ー 8 です。

コマンド デフォルト

デフォルトで、コンフィギュレーション内の最初のメンバーインターフェイスが使用可能な場合、そのインターフェイスがアクティブ インターフェイスとなります。

コマンド履歴

リリース	変更内容
6.1	このコマンドが導入されました。

使用上のガイドライン

Device Manager に冗長インターフェイスを作成します。冗長インターフェイスを作成する場合は、プライマリインターフェイスを指定します。このコマンドを使用して、実行時にアクティブになるインターフェイスを変更します。

どのインターフェイスがアクティブであるかを表示するには、次のコマンドを入力します。

show interface redundant*number* **detail | grep Member**

次に例を示します。

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

例

次の例では、redundant1 インターフェイスのアクティブインターフェイスを変更します。

```
> show interface redundant1 detail | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2

> redundant-interface redundant 1 active-member gigabitethernet0/2
```

関連コマンド

Command	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。

restore

Secure Firewall Management Centerによって管理されている Secure Firewall Threat Defense デバイスからローカルにバックアップされた設定を復元するには、**restore** コマンドを使用します。リモートの場所に保存されたバックアップを復元するには、バックアップファイルの場所とユーザー名に対して追加パラメータを指定します。

restore remote-manager-backup [*backup tar-file* | **location** [*scp-hostname username filepath backup tar-file*]]

構文の説明

remote-manager-backup *backup tar-file*	Secure Firewall Management Center によって作成されたローカルバックアップを復元します。ローカル バックアップ ファイルが Secure Firewall Threat Defense デバイスに保存されます。
remote-manager-backup location *scp-hostname username filepath backup tar-file*	Secure Firewall Management Center によって作成されたリモートバックアップを復元します。リモートバックアップは、ユーザーが設定した場所に保存され、SCP サーバーからアクセスできます。また、ホスト名、ユーザー名、およびファイルパスによって識別されます。

コマンド履歴

リリース	変更内容
6.3	このコマンドが導入されました。

使用上のガイドライン

restore コマンドは、新しい/交換用 Secure Firewall Threat Defense の Secure Firewall Threat Defense システムファイル、Snort DB テーブル、および LINA 実行コンフィギュレーションを復元します。また、**restore** コマンドを使用すると、実際の復元操作を実行する前に、Secure Firewall Threat Defense デバイス上の既存の LINA 実行コンフィギュレーションが削除されます。これにより、Secure Firewall Threat Defense デバイスはバックアップが実行された時点で存在する設定のみを保持します。復元操作が成功すると、交換用デバイスのシリアル番号を除くすべてのデバイス設定が交換されます。

復元操作により、元のデバイスに割り当てられた汎用一意識別子（UUID）を使用して、交換用/新規 Secure Firewall Threat Defense デバイスと元の Secure Firewall Management Center デバイスとの接続が再確立されます。復元が正常に完了すると、Secure Firewall Management Center はデバイスのすべてのポリシーを期限切れとしてマークし、デバイスの交換手順が完了したときに、交換用 Secure Firewall Threat Defense に影響する可能性のある Secure Firewall Management Center の設定変更が展開されるようにします。これにより、新しい Secure Firewall Threat Defense および Secure Firewall Management Center 設定が同期されます。

例

次に、ローカルバックアップファイルからの復元操作の例を示します。

```
> restore remote-manager-backup 10.10.1.168_PRIMARY_20180614055906.tar
```

次に、リモートバックアップファイルからの復元操作の例を示します。

```
>restore remote-manager-backup location 10.106.140.100 admin /Volume/home/admin
10.10.1.168_PRIMARY_20180614055906.tar
```

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。