CHAPTER 22

# packet-tracer コマンド～ pwd コマンド

# packet-tracer

パケット スニッフィングおよびネットワーク障害隔離を実行するパケット トレース機能をイネーブルにするには、特権 EXEC コンフィギュレーション モードで **packet-tracer** コマンドを使用します。パケット キャプチャ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**packet-tracer input** [*src_int*] *protocol src_addr src_port dest_addr dest_port* [**detailed**] [**xml**]

**no packet-tracer**

## 構文の説明

| | |
|---|---|
| **input** *src_int* | パケット トレースの送信元インターフェイスを指定します。 |
| *protocol* | パケット トレースのプロトコル タイプを指定します。使用可能なプロトコル タイプ キーワードは、*icmp*、*rawip*、*tcp*、または *udp* です。 |
| *src_addr* | パケット トレースの送信元アドレスを指定します。 |
| *src_port* | パケット トレースの送信元ポートを指定します。 |
| *dest_addr* | パケット トレースの宛先アドレスを指定します。 |
| *dest_port* | パケット トレースの宛先ポートを指定します。 |
| **detailed** | （任意）パケット トレースの詳細情報を提供します。 |
| **xml** | （任意）トレース キャプチャを XML 形式で表示します。 |

## デフォルト

このコマンドには、デフォルト設定がありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 特権 EXEC モード | • | — | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

パケットのキャプチャに加えて、セキュリティ アプライアン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と、ルールの追加に使用した CLI ラインを表示します。
- 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、およびセキュリティ アプライアンスによるパケットの処理方法を提供します。コンフィギュレーションからのコマンドでパケットがドロップしなかった場合、**packet-tracer** コマンドは、原因に関する情報を判読しやすい方法で提供します。たとえば、無効なヘッダー検証が原因でパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」というメッセージが表示されます。

## 例

内部ホスト 10.2.25.3 から外部ホスト 209.165.202.158 へのパケット トレーシングをイネーブルにし、詳細情報を出力するには、次のように入力します。

```
hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed
```

## 関連コマンド

| コマンド | 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。 |

# page style

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **page style** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

**page style** *value*

[**no**] **page style** *value*

**構文の説明**

| | |
|---|---|
| *value* | Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータ（最大 256 文字）。 |

**デフォルト**

デフォルトのページ スタイルは、background-color:white;font-family:Arial,Helv,sans-serif です。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| webvpn カスタマイゼーション コンフィギュレーション | • | — | • | — | — |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 7.1(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**

**style** オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

**例**

次に、ページ スタイルを large にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# page style font-size:large
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **logo** | WebVPN ページのロゴをカスタマイズします。 |
| **title** | WebVPN ページのタイトルをカスタマイズします。 |

# pager

Telnet セッションで「---more---」プロンプトが表示されるまでの 1 ページあたりのデフォルト行数を設定するには、グローバル コンフィギュレーション モードで **pager** コマンドを使用します。

**pager [lines]** *lines*

## 構文の説明

| | |
|---|---|
| [**lines**] *lines* | 「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。 |

## デフォルト

デフォルトは 24 行です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドは、特権 EXEC モードのコマンドからグローバル コンフィギュレーション モードのコマンドに変更されました。**terminal pager** コマンドが、特権 EXEC モードのコマンドとして追加されました。 |

## 使用上のガイドライン

このコマンドは、Telnet セッションでのデフォルトの pager line 設定を変更します。現在のセッションについてのみ、設定を一時的に変更する場合は、**terminal pager** コマンドを使用します。

管理コンテキストに対して Telnet 接続し、他のコンテキストに変更した場合、そのコンテキストの **pager** コマンドで別の設定が使用される場合でも、pager line 設定はセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

## 例

次に、表示される行数を 20 に変更する例を示します。

```
hostname(config)# pager 20
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure terminal** | 端末の表示幅設定をクリアします。 |
| **show running-config terminal** | 現在の端末設定を表示します。 |
| **terminal** | システム ログ メッセージを Telnet セッションで表示できるようにします。 |
| **terminal pager** | Telnet セッションで「`---more---`」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。 |
| **terminal width** | グローバル コンフィギュレーション モードでの端末の表示幅を設定します。 |

# parameters

パラメータ コンフィギュレーション モードを開始してインスペクション ポリシー マップのパラメータを設定するには、ポリシー マップ コンフィギュレーション モードで **parameters** コマンドを使用します。

**parameters**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ポリシー マップ コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で、**inspect** コマンドを使用してインスペクション エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシー マップで定義されているアクションを、オプションでイネーブルにすることもできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は、インスペクション ポリシー マップの名前です。

インスペクション ポリシー マップは、1 つ以上の **parameters** コマンドをサポートできます。パラメータは、インスペクション エンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

## 例

次に、デフォルトのインスペクション ポリシー マップにおける DNS パケットの最大メッセージ長を設定する例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 512
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップのクラス マップ名を指定します。 |
| **class-map type inspect** | アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。 |
| **policy-map** | レイヤ 3/4 のポリシー マップを作成します。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# participate

デバイスを仮想ロード バランシング クラスタに強制参加させるには、VPN ロード バランシング コンフィギュレーション モードで **participate** コマンドを使用します。クラスタへの参加からデバイスを削除するには、このコマンドの **no** 形式を使用します。

**participate**

**no participate**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作では、デバイスは VPN ロード バランシング クラスタに参加しません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| VPN ロード バランシング コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

まず、**interface** および **nameif** コマンドを使用してインターフェイスを設定し、**vpn load-balancing** コマンドを使用して VPN ロード バランシング モードを開始する必要があります。さらに、**cluster ip** コマンドを使用してクラスタ IP アドレスを設定し、仮想クラスタ IP アドレスが参照するインターフェイスを設定しておく必要があります。

このコマンドは、このデバイスを仮想ロード バランシング クラスタに強制的に参加させます。デバイスへの参加をイネーブルにするには、このコマンドを明示的に発行する必要があります。

クラスタに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。

**（注）** 暗号化を使用するときは、**isakmp enable** *inside* コマンドをあらかじめ設定しておく必要があります。*inside* は、ロード バランシングの内部インターフェイスを指定します。ロード バランシングの内部インターフェイスで isakmp がイネーブルでない場合は、クラスタ暗号化を設定しようとするとエラー メッセージが表示されます。

isakmp が **cluster encryption** コマンドの設定時にはイネーブルで、**participate** コマンドを設定する前にディセーブルになった場合、**participate** コマンドを入力するとエラー メッセージが表示され、ローカル デバイスはクラスタに参加しません。

## 例

次に、現在のデバイスを VPN ロード バランシング クラスタに参加できるようにする **participate** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **vpn load-balancing** | VPN ロード バランシング モードを開始します。 |

# passive-interface

インターフェイスで RIP ルーティング更新の送信をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスで RIP ルーティング更新を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

**passive-interface** {**default** | *if_name*}

**no passive-interface** {**default** | *if_name*}

## 構文の説明

| | |
|---|---|
| **default** | （任意）すべてのインターフェイスを受動モードに設定します。 |
| *if_name* | （任意）指定したインターフェイスをパッシブ モードに設定します。 |

## デフォルト

RIP がイネーブルになると、アクティブ RIP に対してすべてのインターフェイスがイネーブルになります。

インターフェイスまたは **default** キーワードを指定しない場合、コマンドのデフォルトは **default** であり、コンフィギュレーションでは `passive-interface default` として表示されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

インターフェイス上でパッシブ RIP をイネーブルにします。インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルを設定しますが、ルーティング更新はブロードキャストしません。

## 例

次に、外部インターフェイスをパッシブ RIP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、RIP 更新を送受信します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure rip** | 実行コンフィギュレーションからすべての RIP コマンドをクリアします。 |
| **router rip** | RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードを開始します。 |
| **show running-config rip** | 実行コンフィギュレーションの RIP コマンドを表示します。 |

# passive-interface（EIGRP）

インターフェイスで EIGRP ルーティング更新の送受信をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスでルーティング更新を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

**passive-interface** {**default** | *if_name*}

**no passive-interface** {**default** | *if_name*}

## 構文の説明

| | |
|---|---|
| **default** | （任意）すべてのインターフェイスを受動モードに設定します。 |
| *if_name* | （任意）**nameif** コマンドでパッシブ モードに指定したインターフェイスの名前。 |

## デフォルト

そのインターフェイスでルーティングがイネーブルになると、アクティブ ルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスがイネーブルになります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| ルータ コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(1) | このコマンドが導入されました。 |
| 8.0(2) | EIGRP ルーティングのサポートが追加されました。 |

## 使用上のガイドライン

インターフェイス上でパッシブ ルーティングをイネーブルにします。EIGRP の場合は、これによりそのインターフェイスでのルーティング更新の送受信がディセーブルになります。

EIGRP コンフィギュレーションでは、複数の **passive-interface** コマンドを使用できます。**passive-interface default** コマンドを使用してすべてのインターフェイスで EIGRP ルーティングをディセーブルにし、次に **no passive-interface** コマンドを使用して特定インターフェイスで EIGRP ルーティングをイネーブルにすることが可能です。

## 例

次に、外部インターフェイスをパッシブ EIGRP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、EIGRP 更新を送受信します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

次に、内部インターフェイスを除くすべてのインターフェイスをパッシブ EIGRP に設定する例を示します。内部インターフェイスのみが EIGRP 更新を送受信します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface default
hostname(config-router)# no passive-interface inside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show running-config router** | 実行コンフィギュレーションに含まれるルータ コンフィギュレーション コマンドを表示します。 |

# passwd

ログイン パスワードを設定するには、グローバル コンフィギュレーション モードで **passwd** コマンドを使用します。パスワードをデフォルトの「cisco」に戻すには、このコマンドの **no** 形式を使用します。Telnet または SSH を使用してデフォルト ユーザとして CLI にアクセスするときに、ログイン パスワードを求められます。ログイン パスワードを入力すると、ユーザ EXEC モードが開始されます。

{**passwd** | **password**} *password* [**encrypted**]

**no** {**passwd** | **password**} *password*

## 構文の説明

| | |
|---|---|
| encrypted | （任意）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるが、元のパスワードがわからない場合、暗号化されたパスワードとこのキーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力するときにだけ表示されます。 |
| **passwd** \| **password** | どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。 |
| *password* | パスワードを最大 80 文字のストリングで設定します。大文字と小文字は区別されます。パスワードにスペースを含めることはできません。 |

## デフォルト

デフォルトのパスワードは「cisco」です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

このログイン パスワードは、デフォルト ユーザのものです。**aaa authentication console** コマンドを使用して Telnet または SSH のユーザごとに CLI 認証を設定する場合、このパスワードは使用されません。

## 例

次に、パスワードを Pa$$w0rd に設定する例を示します。

```
hostname(config)# passwd Pa$$w0rd
```

次に、パスワードを別のセキュリティ アプライアンスからコピーした暗号化されたパスワードに設定する例を示します。

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure passwd** | ログイン パスワードをクリアします。 |
| **enable** | 特権 EXEC モードを開始します。 |
| **enable password** | イネーブル パスワードを設定します。 |
| **show curpriv** | 現在ログインしているユーザ名とユーザの特権レベルを表示します。 |
| **show running-config passwd** | 暗号化された形式でログイン パスワードを表示します。 |

# password（クリプト CA トラスト ポイント）

登録時に CA に登録されたチャレンジ フレーズを指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **password** コマンドを使用します。通常、CA はこのフレーズを使用して、その後の失効要求を認証します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**password** *string*

**no password**

## 構文の説明

| | |
|---|---|
| *string* | パスワードの名前をストリングとして指定します。最初の文字を数値にはできません。ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字 - スペース - 任意の文字の形式ではパスワードを指定できません。数字の後にスペースを使用すると、問題が発生します。たとえば、「hello 21」は適切なパスワードですが、「21 hello」はそうではありません。パスワード チェックでは、大文字と小文字が区別されます。たとえば、パスワード「Secret」は、パスワード「secret」とは異なります。 |

## デフォルト

デフォルト設定では、パスワードを含めません。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| クリプト CA トラストポイント コンフィギュレーション | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書失効パスワードを指定できます。指定されたパスワードは、更新されたコンフィギュレーションがセキュリティ アプライアンスによって NVRAM に書き込まれるときに暗号化されます。

このコマンドがイネーブルの場合、証明書登録時にパスワードを求められません。

## 例

次に、トラストポイント central に対してクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に対する登録要求で CA に登録されたチャレンジ フレーズを指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **crypto ca trustpoint** | トラストポイント コンフィギュレーション モードを開始します。 |
| **default enrollment** | 登録パラメータをデフォルト値に戻します。 |

# password-management

パスワード管理をイネーブルにするには、トンネル グループ一般属性コンフィギュレーション モードで **password-management** コマンドを使用します。パスワード管理をディセーブルにするには、このコマンドの **no** 形式を使用します。日数をデフォルト値にリセットするには、このコマンドの **no** 形式を使用し、**password-expire-in-days** キーワードを指定します。

**password-management** [**password-expire-in-days** *days*]

**no password-management**

**no password-management password-expire-in-days** [*days*]

## 構文の説明

| | |
|---|---|
| *days* | 現行のパスワードが失効するまでの日数（0 ～ 180）を指定します。**password-expire-in-days** キーワードを指定する場合は、このパラメータは必須です。 |
| **password-expire-in-days** | （任意）直後のパラメータが、セキュリティ アプライアンスでユーザに対して失効が迫っている警告を開始してから、現行のパスワードが失効するまでの日数を指定していることを示します。このオプションは、LDAP サーバに対してのみ有効です。詳細については、「Usage Notes」を参照してください。 |

## デフォルト

このコマンドを指定しない場合は、パスワード管理が発生しません。**password-expire-in-days** キーワードを指定しない場合、現行のパスワードが失効する前に警告を開始するデフォルトの期間は、14 日です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ一般属性コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(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

セキュリティ アプライアンスでは、RADIUS および LDAP プロトコルのパスワード管理をサポートします。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPSec リモート アクセスおよび SSL VPN トンネル グループのパスワード管理を設定できます。

password-management コマンドを設定すると、セキュリティ アプライアンスは、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それからセキュリティ アプライアンスは、ユーザがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザはそのパスワードを使用してログインし続けることができます。

このコマンドは、そのような通知をサポートする AAA サーバに対して有効です。RADIUS または LDAP 認証が設定されていない場合、セキュリティ アプライアンスではこのコマンドが無視されます。

**（注）** MSCHAP をサポートする一部の RADIUS サーバは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。

セキュリティ アプライアンスのリリース 7.1 以降では通常、LDAP による認証時、または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント
- IPSec VPN クライアント
- クライアントレス SSL VPN

Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポート*されません*。RADIUS サーバ（Cisco ACS など）は、認証要求を別の認証サーバにプロキシする場合があります。ただし、セキュリティ アプライアンスからは RADIUS サーバのみに対して通信しているように見えます。

**（注）** LDAP でパスワードを変更するには、市販の LDAP サーバごとに独自の方法が使用されています。現在、セキュリティ アプライアンスでは Microsoft Active Directory および Sun LDAP サーバに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

このコマンドは、パスワードが失効するまでの日数を変更するものではなく、セキュリティ アプライアンスがユーザに対してパスワード失効の警告を開始してから失効するまでの日数を変更するものである点に注意してください。

**password-expire-in-days** キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。セキュリティ アプライアンスは、ユーザに対して失効が迫っていることを通知しませんが、失効後にユーザはパスワードを変更できます。

## 例

次に、WebVPN トンネル グループ「testgroup」について、ユーザに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数を 90 に設定する例を示します。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# password-management password-expire-in-days 90
hostname(config-tunnel-general)#
```

次に、IPSec リモート アクセス トンネル グループ「QAgroup」について、ユーザに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数としてデフォルトの 14 日を使用する例を示します。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
```

```
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure passwd** | ログイン パスワードをクリアします。 |
| **passwd** | ログイン パスワードを設定します。 |
| **radius-with-expiry** | RADIUS 認証時のパスワード更新のネゴシエーションをイネーブルにします（廃止）。 |
| **show running-config passwd** | 暗号化された形式でログイン パスワードを表示します。 |
| **tunnel-group general-attributes** | トンネル グループ一般属性値を設定します。 |

# password-parameter

SSO 認証用のユーザ パスワードを送信する HTTP POST 要求パラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **password-parameter** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

**password-parameter** *string*

（注）　HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

## 構文の説明

| | |
|---|---|
| *string* | HTTP POST 要求に含まれるパスワード パラメータの名前。パスワードの最大長は 128 文字です。 |

## デフォルト

デフォルトの値や動作はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| AAA サーバ ホスト コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(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

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、認証 Web サーバにシングル サインオン認証要求を送信します。必須のコマンド **password-parameter** では、POST 要求に SSO 認証用のユーザ パスワード パラメータを含める必要があることを指定します。

（注）　ユーザは、ログイン時に実際のパスワード値を入力します。このパスワード値は POST 要求に入力され、認証 Web サーバに渡されます。

## 例

次に、AAA サーバ ホスト コンフィギュレーション モードで、user_password という名前のパスワード パラメータを指定する例を示します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# password-parameter user_password
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **action-uri** | シングル サインオン認証用のユーザ名およびパスワードを受信するための Web サーバ URI を指定します。 |
| **auth-cookie-name** | 認証クッキーの名前を指定します。 |
| **hidden-parameter** | 認証 Web サーバと交換するための非表示パラメータを作成します。 |
| **start-url** | プリログイン クッキーを取得する URL を指定します。 |
| **user-parameter** | SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。 |

# password-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **password-prompt** コマンドを使用します。

**password-prompt** {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

## 構文の説明

| | |
|---|---|
| **text** | テキストを変更することを指定します。 |
| **style** | スタイルを変更することを指定します。 |
| *value* | 実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。 |

## デフォルト

パスワード プロンプトのデフォルト テキストは、「PASSWORD:」です。

パスワード プロンプトのデフォルト スタイルは、color:black;font-weight:bold;text-align:right です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| WebVPN カスタマイゼーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(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

**style** オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

**（注）** WebVPN ページを簡単にカスタマイズするには、ASDM を使用することを推奨します。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するための便利な機能があります。

## 例

次に、テキストを「Corporate Password:」に変更し、フォントのウェイトを太くするようにデフォルト スタイルを変更する例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# password-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# password-prompt style font-weight:bolder
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **group-prompt** | WebVPN ページのグループ プロンプトをカスタマイズします。 |
| **username-prompt** | WebVPN ページのユーザ名プロンプトをカスタマイズします。 |

# password-storage

ユーザがクライアント システムに各自のログイン パスワードを保管できるようにするには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **password-storage enable** コマンドを使用します。パスワードの保管をディセーブルにするには、**password-storage disable** コマンドを使用します。

実行コンフィギュレーションから password-storage 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーから password-storage 値を継承できます。

**password-storage {enable | disable}**

**no password-storage**

## 構文の説明

| | |
|---|---|
| **disable** | パスワードの保管をディセーブルにします。 |
| **enable** | パスワードの保管をイネーブルにします。 |

## デフォルト

パスワードの保管はディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グループ ポリシー | • | — | • | — | — |
| ユーザ名 | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

セキュア サイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザ認証には関係ありません。

## 例

次に、FirstGroup という名前のグループ ポリシーに対してパスワードの保管をイネーブルにする例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

# peer-id-validate

ピアの証明書を使用してピアの ID を検証するかどうかを指定するには、トンネル グループ IPSec 属性モードで **peer-id-validate** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**peer-id-validate** *option*

**no peer-id-validate**

## 構文の説明

| | |
|---|---|
| *option* | 次のいずれかのオプションを指定します。<br>• **req**：必須<br>• **cert**：証明書でサポートされる場合<br>• **nocheck**：チェックしない |

## デフォルト

このコマンドのデフォルト設定は、**req** です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ ipsec 属性 | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0.1 | このコマンドが導入されました。 |

## 使用上のガイドライン

この属性は、すべての IPSec トンネル グループ タイプに適用できます。

## 例

次に、設定 IPSec コンフィギュレーション モードで、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループ用のピア証明書の ID を使用してピアの検証を要求する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear-configure tunnel-group** | 設定されているすべてのトンネル グループをクリアします。 |

| コマンド | 説明 |
|---|---|
| **show running-config tunnel-group** | すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group ipsec-attributes** | このグループのトンネル グループ ipsec 属性を設定します。 |

# perfmon

パフォーマンス情報を表示するには、特権 EXEC モードで **perfmon** コマンドを使用します。

**perfmon** {**verbose** | **interval** *seconds* | **quiet** | **settings**} [*detail*]

## 構文の説明

| | |
|---|---|
| **verbose** | パフォーマンス モニタ情報をセキュリティ アプライアンス コンソールに表示します。 |
| **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。 |
| **quiet** | パフォーマンス モニタ表示をディセーブルにします。 |
| **settings** | 間隔、および quiet と verbose のどちらであるかを表示します。 |
| *detail* | パフォーマンスに関する詳細情報を表示します。 |

## デフォルト

*seconds* は 120 秒です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 特権 EXEC | • | • | • | • | |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。 |
| 7.2(1) | **detail** キーワードのサポートが追加されました。 |

## 使用上のガイドライン

**perfmon** コマンドを使用すると、セキュリティ アプライアンスのパフォーマンスをモニタできます。**show perfmon** コマンドを使用すると、ただちに情報が表示されます。**perfmon verbose** コマンドを使用すると、2 分間隔で継続して情報が表示されます。**perfmon interval** *seconds* コマンドと **perfmon verbose** コマンドを組み合わせて使用すると、指定した秒数の間隔で継続して情報が表示されます。

次に、パフォーマンス情報の表示例を示します。

| PERFMON STATS: | Current | Average |
|---|---|---|
| Xlates | 33/s | 20/s |
| Connections | 110/s | 10/s |
| TCP Conns | 50/s | 42/s |
| WebSns Req | 4/s | 2/s |
| TCP Fixup | 20/s | 15/s |
| HTTP Fixup | 5/s | 5/s |

| | | |
|---|---|---|
| FTP Fixup | 7/s | 4/s |
| AAA Authen | 10/s | 5/s |
| AAA Author | 9/s | 5/s |
| AAA Account | 3/s | 3/s |

この情報には、毎秒発生する変換数、接続数、Websense 要求数、アドレス変換数（フィックスアップ数）、AAA トランザクション数が示されます。

## 例

次に、パフォーマンス モニタ統計情報を 30 秒間隔でセキュリティ アプライアンス コンソールに表示する例を示します。

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **show perfmon** | パフォーマンス情報を表示します。 |

# periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーション モードで **periodic** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

**periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*

**no periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*

## 構文の説明

| | |
|---|---|
| days-of-the-week | （任意）1 番めの days-of-the-week 引数は、関連付けられている時間範囲の有効範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。<br>この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。<br>• daily：月曜日～日曜日<br>• weekdays：月曜日～金曜日<br>• weekend：土曜日と日曜日<br>終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。 |
| *time* | 時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時です。午後 8 時は 20:00 と指定します。 |
| **to** | 「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。 |

## デフォルト

**periodic** コマンドで値を入力しない場合は、セキュリティ アプライアンスへのアクセスが **time-range** コマンドで定義されたとおりにただちに有効になり、常に有効になります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 時間範囲コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

時間ベース ACL を実装するには、**time-range** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドとともに使用して、時間範囲を ACL にバインドします。

**periodic** コマンドは、時間範囲が有効になるタイミングを指定する 1 つの方法です。**absolute** コマンドを使用して絶対時間範囲を指定する、という別の方法もあります。**time-range** グローバル コンフィギュレーション コマンドで時間範囲の名前を指定した後に、これらのコマンドのいずれかを使用します。**time-range** コマンド 1 つあたり複数の **periodic** エントリを使用できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

**time-range** コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは **absolute start** 時刻を経過した後にのみ評価の対象になり、**absolute end** 時刻を経過した後は評価の対象にはなりません。

時間範囲機能は、セキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

## 例

次に例をいくつか示します。

| 必要な設定 | 入力内容 |
|---|---|
| 月曜～金曜、午前 8 時～ 午後 6 時 only | **periodic weekdays 8:00 to 18:00** |
| 毎日、午前 8 時～ 午後 6 時 only | **periodic daily 8:00 to 18:00** |
| 月曜日午前 8:00 ～ 金曜日午前 8:00 の毎分 | **periodic monday 8:00 to friday 20:00** |
| 週末（土曜日の朝～日曜日の夜） | **periodic weekend 00:00 to 23:59** |
| 土曜日と日曜日の正午～深夜 | **periodic weekend 12:00 to 23:59** |

次に、月曜日から金曜日の午前 8:00 ～ 午後 6:00 に、セキュリティ アプライアンスへのアクセスを 許可する 例を示します。

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

次に、特定の曜日（月曜日、火曜日、および金曜日）の午前 10:30 ～午後 12:30 に、セキュリティ アプライアンスへのアクセスを許可する 例を示します。

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **absolute** | 時間範囲が有効になる絶対時間を定義します。 |
| access-list extended | セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。 |
| **default** | **time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。 |
| **time-range** | 時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。 |

# permit errors

無効な GTP パケットを許可するか、または許可しないと解析が失敗してドロップされるパケットを許可するには、GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用します。このモードには **gtp-map** コマンドを使用してアクセスします。デフォルトの動作（無効なパケットまたは解析中に失敗したパケットはすべてドロップされる）に戻すには、このコマンドの **no** 形式を使用します。

**permit errors**

**no permit errors**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、無効なパケットまたは解析中に失敗したパケットはすべてドロップされます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| GTP マップ コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用すると、無効なパケットやメッセージのインスペクション中にエラーが発生したパケットをドロップするのではなく、セキュリティ アプライアンス経由で送信することができます。

## 例

次に、解析中に無効なパケットや失敗したパケットを含むトラフィックを許可する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear service-policy inspect gtp** | グローバルな GTP 統計情報をクリアします。 |
| **gtp-map** | GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。 |

| コマンド | 説明 |
|---|---|
| **inspect gtp** | アプリケーション インスペクションに使用する特定の GTP マップを適用します。 |
| **permit response** | ロード バランシング GSN をサポートします。 |
| **show service-policy inspect gtp** | GTP コンフィギュレーションを表示します。 |

# permit response

ロード バランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。このモードには **gtp-map** コマンドを使用してアクセスします。セキュリティ アプライアンスで要求の送信先ホスト以外の GSN から GTP 応答をドロップできるようにするには、このコマンドの **no** 形式を使用します。

**permit response to-object-group** *to_obj_group_id* **from-object-group** *from_obj_group_id*

**no permit response to-object-group** *to_obj_group_id* **from-object-group** *from_obj_group_id*

## 構文の説明

| | |
|---|---|
| **from-object-group** *from_obj_group_id* | **object-group** コマンドを使用して設定されたオブジェクト グループの名前を指定します。このオブジェクト グループは、*to_obj_group_id* 引数で指定されたオブジェクト グループ内の GSN セットに応答を送信できます。セキュリティ アプライアンスは、IPv4 アドレスを持つネットワークオブジェクトが含まれたオブジェクトグループのみをサポートしています。現在、IPv6 アドレスは GTP ではサポートされていません。 |
| **to-object-group** *to_obj_group_id* | **object-group** コマンドを使用して設定されたオブジェクト グループの名前を指定します。このオブジェクト グループは、*from_obj_group_id* 引数で指定されたオブジェクト グループ内の GSN セットから応答を受信できます。セキュリティ アプライアンスは、IPv4 アドレスを持つネットワークオブジェクトが含まれたオブジェクトグループのみをサポートしています。現在、IPv6 アドレスは GTP ではサポートされていません。 |

## デフォルト

デフォルトでは、セキュリティ アプライアンスは、要求の送信先ホスト以外の GSN から GTP 応答をドロップします。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| GTP マップ コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0（4） | このコマンドが導入されました。 |

## 使用上のガイドライン

ロード バランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。**permit response** コマンドは、GTP 応答の送信先とは異なる GSN からの応答を許可するように GTP マップを設定します。

ロードバランシング GSN のプールは、ネットワーク オブジェクトとして指定します。同様に、SGSN もネットワーク オブジェクトとして指定します。応答している GSN が GTP 要求の送信先の GSN と同じオブジェクト グループに属している場合、および応答している GSN による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN がある場合、セキュリティ アプライアンスはその応答を許可します。

## 例

次に、192.168.32.0 ネットワーク上の任意のホストから IP アドレス 192.168.112.57 のホストへの GTP 応答を許可する例を示します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group gsnpool32
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear service-policy inspect gtp** | グローバルな GTP 統計情報をクリアします。 |
| **gtp-map** | GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。 |
| **inspect gtp** | アプリケーション インスペクションに使用する特定の GTP マップを適用します。 |
| **permit errors** | 無効な GTP パケットを許可します。 |
| **show service-policy inspect gtp** | GTP コンフィギュレーションを表示します。 |

# pfs

PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS をディセーブルにするには、**pfs disable** コマンドを使用します。実行コンフィギュレーションから PFS 属性を削除するには、このコマンドの **no** 形式を使用します。

**pfs {enable | disable}**

**no pfs**

## 構文の説明

| | |
|---|---|
| **disable** | PFS をディセーブルにします。 |
| **enable** | PFS をイネーブルにします。 |

## デフォルト

PFS はディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グループ ポリシー コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

VPN クライアントとセキュリティ アプライアンスの PFS 設定は一致する必要があります。

別のグループ ポリシーから PFS の値を継承できるようにするには、このコマンドの **no** 形式を使用します。

IPSec ネゴシエーションでは、PFS により、新しい各暗号キーはそれまでのあらゆるキーと無関係であることが保証されます。

## 例

次に、FirstGroup という名前のグループ ポリシーに対して PFS を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# pfs enable
```

# phone-proxy

電話プロキシ インスタンスを設定するには、グローバル コンフィギュレーション モードで **phone-proxy** コマンドを使用します。

電話プロキシ インスタンスを削除するには、このコマンドの **no** 形式を使用します。

**phone-proxy** *phone_proxy_name*

**no phone-proxy** *phone_proxy_name*

## 構文の説明

| | |
|---|---|
| *phone_proxy_name* | Phone Proxy インスタンスの名前を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

セキュリティ アプライアンスでは、電話プロキシ インスタンスを 1 つだけ設定できます。

HTTP プロキシ サーバ用に NAT が設定されている場合、IP 電話に関する HTTP プロキシ サーバのグローバルまたはマッピング IP アドレスは、電話プロキシ コンフィギュレーション ファイルに書き込まれます。

## 例

次に、**phone-proxy** コマンドを使用して、電話プロキシ インスタンスを設定する例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
hostname(config-phone-proxy)# media-termination address 128.106.254.3
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
hostname(config-phone-proxy)# timeout secure-phones 00:05:00
hostname(config-phone-proxy)# disable service-settings
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **ctl-file（グローバル）** | Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。 |
| **ctl-file（Phone-Proxy）** | Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。 |
| **tls-proxy** | TLS プロキシ インスタンスを設定します。 |

# pim

インターフェイス上で PIM を再びイネーブルにするには、インターフェイス コンフィギュレーション モードで **pim** コマンドを使用します。PIM をディセーブルにするには、このコマンドの **no** 形式を使用します。

**pim**

**no pim**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM をイネーブルにします。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM をイネーブルにします。**pim** コマンドの **no** 形式のみが、コンフィギュレーションに保存されます。

**（注）** PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

## 例

次に、選択したインターフェイスで PIM をディセーブルにする例を示します。

```
hostname(config-if)# no pim
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim accept-register

PIM 登録メッセージをフィルタリングするようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **pim accept-register** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

**pim accept-register** {**list** *acl* | **route-map** *map-name*}

**no pim accept-register**

## 構文の説明

| | |
|---|---|
| **list** *acl* | アクセス リストの名前または番号を指定します。このコマンドでは、拡張ホスト ACL のみを使用します。 |
| **route-map** *map-name* | ルート マップ名を指定します。参照されるルート マップでは、拡張ホスト ACL を使用します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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、不正な送信元を RP に登録できないようにするために使用します。不正な送信元が RP に登録メッセージを送信すると、セキュリティ アプライアンスはただちに登録停止メッセージを送り返します。

## 例

次に、「no-ssm-range」という名前のアクセス リストで定義された送信元からの PIM 登録メッセージを制限する例を示します。

```
hostname(config)# pim accept-register list no-ssm-range
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim bidir-neighbor-filter

DF 選出に参加できる双方向対応ネイバーを制御するには、インターフェイス コンフィギュレーション モードで **pim bidir-neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

**pim bidir-neighbor-filter** *acl*

**no pim bidir-neighbor-filter** *acl*

## 構文の説明

| | |
|---|---|
| *acl* | アクセス リストの名前または番号を指定します。アクセス リストは、双方向 DF 選出に参加できるネイバーを定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。 |

## デフォルト

すべてのルータは双方向対応であると見なされます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

**pim bidir-neighbor-filter** コマンドを使用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。この場合、すべてのルータのスパース モード ドメインへの参加を許可しながら、DF 選出へ参加しなければならないルータを指定します。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

**pim bidir-neighbor-filter** コマンドがイネーブルの場合、ACL で許可されているルータは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

## 例

次に、10.1.1.1 を PIM 双方向ネイバーにできる例を示します。

```
hostname(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
hostname(config)# access-list bidir_test deny any
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter bidir_test
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast boundary** | 管理上有効範囲が設定されたマルチキャスト アドレスに対してマルチキャスト境界を定義します。 |
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim dr-priority

指定ルータ選出に使用されるセキュリティ アプライアンスでネイバーのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

**pim dr-priority** *number*

**no pim dr-priority**

## 構文の説明

| | |
|---|---|
| *number* | 0 ～ 4294967294 までの数字。この番号は、指定ルータを決定するときにデバイスのプライオリティを判断するために使用されます。0 を指定すると、セキュリティ アプライアンスは指定ルータになりません。 |

## デフォルト

デフォルト値は、1 です

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

インターフェイスでプライオリティ値が最大のデバイスが PIM 指定ルータになります。複数のデバイスで指定ルータのプライオリティが同じである場合は、IP アドレスが最大のデバイスが DR になります。デバイスの hello メッセージに DR-Priority Option が含まれていない場合は、プライオリティが最大のデバイスとして扱われ、指定ルータになります。複数のデバイスで hello メッセージにこのオプションが含まれていない場合は、IP アドレスが最大のデバイスが指定ルータになります。

## 例

次に、インターフェイスの DR プライオリティを 5 に設定する例を示します。

```
hostname(config-if)# pim dr-priority 5
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim hello-interval

PIM hello メッセージの頻度を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello-interval をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**pim hello-interval** *seconds*

**no pim hello-interval** [*seconds*]

## 構文の説明

| | |
|---|---|
| *seconds* | セキュリティ アプライアンスが hello メッセージを送信するまでの待機秒数。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 30 秒です。 |

## デフォルト

30 秒

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |

## 例

次に、PIM hello 間隔を 1 分に設定する例を示します。

```
hostname(config-if)# pim hello-interval 60
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim join-prune-interval

PIM Join/Prune の間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**pim join-prune-interval** *seconds*

**no pim join-prune-interval** [*seconds*]

## 構文の説明

| | |
|---|---|
| *seconds* | セキュリティ アプライアンスが Join/Prune メッセージを送信するまでの待機秒数。有効な値の範囲は、10 ～ 600 秒です。デフォルトは 60 秒です。 |

## デフォルト

60 秒

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |

## 例

次に、PIM Join/Prune 間隔を 2 分に設定する例を示します。

```
hostname(config-if)# pim join-prune-interval 120
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim neighbor-filter

PIM に参加できる隣接ルータを制御するには、インターフェイス コンフィギュレーション モードで **pim neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

**pim neighbor-filter** *acl*

**no pim neighbor-filter** *acl*

## 構文の説明

| | |
|---|---|
| *acl* | アクセス リストの名前または番号を指定します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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、PIM に参加できる隣接ルータを定義します。このコマンドがコンフィギュレーションに存在しない場合、制限はありません。

コンフィギュレーションでこのコマンドを使用するには、マルチキャスト ルーティングおよび PIM がイネーブルである必要があります。マルチキャスト ルーティングをディセーブルにすると、このコマンドはコンフィギュレーションから削除されます。

## 例

次に、IP アドレスが 10.1.1.1 であるルータをインターフェイス GigabitEthernet0/2 で PIM ネイバーにする例を示します。

```
hostname(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
hostname(config)# access-list pim_filter deny any
hostname(config)# interface gigabitEthernet0/2
hostname(config-if)# pim neighbor-filter pim_filter
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim old-register-checksum

古いレジスタ チェックサム方式を使用するランデブー ポイント（RP）での下位互換性を保つには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠レジスタを生成するには、このコマンドの **no** 形式を使用します。

**pim old-register-checksum**

**no pim old-register-checksum**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

セキュリティ アプライアンス は PIM RFC 準拠レジスタを生成します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

セキュリティ アプライアンス ソフトウェアは、Cisco IOS 方式を使用せずに、PIM ヘッダーにチェックサムのあるレジスタ メッセージとそれに続く 4 バイトのみを受け入れます。つまり、すべての PIM メッセージ タイプについて PIM メッセージ全体を含むレジスタ メッセージを受け入れます。**pim old-register-checksum** コマンドを使用すると、Cisco IOS ソフトウェアと互換性のあるレジスタが生成されます。

## 例

次に、古いチェックサム計算を使用するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# pim old-register-checksum
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# pim rp-address

PIM ランデブー ポイント（RP）のアドレスを使用するには、グローバル コンフィギュレーション モードで **pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

**pim rp-address** *ip_address* [*acl*] [**bidir**]

**no pim rp-address** *ip_address*

## 構文の説明

| | |
|---|---|
| *acl* | （任意）RP とともに使用されるマルチキャスト グループを定義する標準アクセス リストの名前または番号。このコマンドではホスト ACL を使用しないでください。 |
| **bidir** | （任意）指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定せずにコマンドを設定した場合、指定したグループは PIM スパース モードで動作します。 |
| *ip_address* | PIM RP になるルータの IP アドレス。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。 |

## デフォルト

PIM RP アドレスは設定されていません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

一般的な PIM Sparse Mode（PIM-SM; PIM スパース モード）内または双方向ドメイン内にあるすべてのルータは、既知の PIM RP アドレスを認識する必要があります。アドレスは、このコマンドを使用してスタティックに設定されます。

**（注）** セキュリティ アプライアンス では、Auto-RP をサポートしません。**pim rp-address** コマンドを使用して、RP アドレスを指定する必要があります。

複数のグループにサービスを提供するように単一の RP を設定できます。アクセス リストに指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。アクセス リストを指定しない場合、グループの RP は IP マルチキャスト グループの範囲（224.0.0.0/4）全体に適用されます。

（注）　セキュリティ アプライアンスは、実際の双方向コンフィギュレーションとは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

## 例

次に、すべてのマルチキャスト グループに対して PIM RP アドレスを 10.0.0.1 に設定する例を示します。

```
hostname(config)# pim rp-address 10.0.0.1
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **pim accept-register** | PIM レジスタ メッセージをフィルタリングするように候補 RP を設定します。 |

# pim spt-threshold infinity

常に共有ツリーを使用し、Shortest-Path Tree（SPT; 最短パス ツリー）スイッチオーバーを実行しないようにラスト ホップ ルータの動作を変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**pim spt-threshold infinity** [**group-list** *acl*]

**no pim spt-threshold**

## 構文の説明

| | |
|---|---|
| **group-list** *acl* | （任意）送信元グループはアクセス リストによって制限されていることを示します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされません。 |

## デフォルト

ラスト ホップ PIM ルータは、デフォルトで最短パスの送信元に切り替わります。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

**group-list** キーワードを使用しない場合、このコマンドはすべてのマルチキャスト グループに適用されます。

## 例

次に、最短パス送信元ツリーに切り替えるのではなく、常に共有ツリーを使用するようにラスト ホップ PIM ルータを設定する例を示します。

```
hostname(config)# pim spt-threshold infinity
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **multicast-routing** | セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにします。 |

# ping

他の IP アドレスがセキュリティ アプライアンスから認識できるかどうかを判断するには、特権 EXEC モードで **ping** コマンドを使用します。

**ping** [*if_name*] *host* [**data** *pattern*] [**repeat** *count*] [**size** *bytes*] [**timeout** *seconds*] [**validate**]

## 構文の説明

| | |
|---|---|
| **data** *pattern* | （任意）16 進数による 16 ビットのデータ パターンを指定します。 |
| *host* | ping の送信先ホストの IPv4 アドレス、IPv6 アドレス、または名前。名前は DNS 名、または **name** コマンドで割り当てた名前です。DNS 名の最大文字数は 128、**name** コマンドで作成した名前の最大文字数は 63 です。 |
| *if_name* | （任意）*host* がアクセス可能なインターフェイス名を指定します。インターフェイス名は、**nameif** コマンドで設定します。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。 |
| **repeat** *count* | （任意）ping 要求を繰り返す回数を指定します。 |
| **size** *bytes* | （任意）データグラム サイズをバイト数で指定します。 |
| **timeout** *seconds* | （任意）ping 要求がタイムアウトするまでの秒数を指定します。 |
| **validate** | （任意）応答データを検証するように指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 特権 EXEC | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |
| 7.2(1) | DNS 名のサポートが追加されました。 |

## 使用上のガイドライン

**ping** コマンドを使用すると、セキュリティ アプライアン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。セキュリティ アプライアンスに接続できる場合は、**icmp permit any** *interface* コマンドが設定されていることを確認します。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、セキュリティ アプライアン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。

```
hostname(config)# 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)
```

セキュリティ アプライアンス 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。指定した *if_name* の名前は、ping の送信元アドレスとして使用されます。

内部ホストから外部ホストに対して ping を送信するには、次のいずれかの手順を実行します。

- エコー応答の場合は、ICMP **access-list** コマンドを使用します。たとえば、すべてのホストに対して ping アクセスを与えるには、**access-list acl_grp permit icmp any any** コマンドを使用し、**access-group** コマンドを使用してテストするインターフェイスに対して **access-list** コマンドをバインドします。
- **inspect icmp** コマンドを使用して ICMP インスペクション エンジンを設定します。たとえば、**inspect icmp** コマンドをグローバル サービス ポリシーの **class default_inspection** クラスに追加すると、内部ホストによって開始されるエコー要求に対して、エコー応答はセキュリティ アプライアンスを通過できます。

拡張された ping を実行することもできます。この場合、キーワードを一度に 1 行ずつ入力できます。

ホストやルータの間でセキュリティ アプライアンスを通過して ping を実行し、ping が成功しない場合、**capture** コマンドを使用して ping が成功するかどうかをモニタします。

セキュリティ アプライアンスの **ping** コマンドでは、インターフェイス名を必要としません。インターフェイス名を指定しない場合、指定したアドレスを探すためにセキュリティ アプライアンスはルーティング テーブルをチェックします。ICMP エコー要求の送信に使用されるインターフェイスを示すために、インターフェイス名を指定できます。

## 例

次に、他の IP アドレスがセキュリティ アプライアンスから認識できるかどうかを判断する例を示します。

```
hostname# 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
```

次に、DNS 名を使用してホストを指定する例を示します。

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

次に、拡張された ping を使用する例を示します。

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
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
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| capture | インターフェイスでパケットをキャプチャします。 |
| icmp | インターフェイスが終端となる ICMP トラフィックのアクセス ルールを設定します。 |
| **show interface** | VLAN コンフィギュレーションの情報を表示します。 |

# police

QoS ポリシングをクラス マップに適用するには、クラス コンフィギュレーション モードで **police** コマンドを使用します。レート制限の要件を削除するには、このコマンドの **no** 形式を使用します。ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1 つのトラフィック フローが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、セキュリティ アプライアンスは超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

**police** {**output** | **input**} *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]

**no police**

## 構文の説明

| | |
|---|---|
| *conform-burst* | 適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。 |
| **conform-action** | レートが *conform_burst* 値を下回ったときに実行するアクションを設定します。 |
| *conform-rate* | このトラフィック フローのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。 |
| **drop** | パケットをドロップします。 |
| **exceed-action** | レートが *conform-rate* 値～ *conform-burst* 値の範囲にあるときに実行するアクションを設定します。 |
| **input** | 入力方向のトラフィック フローのポリシングをイネーブルにします。 |
| **output** | 出力方向のトラフィック フローのポリシングをイネーブルにします。 |
| **transmit** | パケットを送信します。 |

## デフォルト

デフォルトの動作や変数はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| クラス コンフィギュレーション | • | • | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.2(1) | **input** オプションが追加されました。着信方向のトラフィックのポリシングがサポートされます。 |

**使用上のガイドライン**

ポリシングをイネーブルにするには、Modular Policy Framework を使用して次のように設定します。

1. **class-map**：ポリシングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **police**：クラス マップのポリシングをイネーブルにします。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

**（注）** **police** コマンドは、最大速度および最大バースト レートを強制し、それらの値を適合レート値に強制的にあわせるだけです。**conform-action** または **exceed-action** の指定は、存在する場合でも適用されません。

**（注）** conform-burst パラメータが省略された場合のデフォルト値は conform-rate のバイト数の 1/32 です（つまり、conform-rate が 100,000 の場合、conform-burst のデフォルト値は 100,000/32 = 3,125 です）。conform-rate の単位はビット / 秒で、conform-burst の単位はバイト数です。

セキュリティ アプライアンスで必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能をセキュリティ アプライアンスに設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティ キューイング（特定のトラフィックについて）+ ポリシング（その他のトラフィックについて）

  同じトラフィックのセットに対して、プライオリティ キューイングとポリシングを両方設定することはできません。

- トラフィック シェーピング（1 つのインターフェイス上のすべてのトラフィック）+ 階層型プライオリティ キューイング（トラフィックのサブセット）。

通常、トラフィック シェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定はセキュリティ アプライアンスでは制限されていません。

確立済みの VPN クライアント /LAN-to-LAN または非トンネル トラフィックが存在するインターフェイスに対して、サービス ポリシーが適用または削除されると、トラフィック ストリームに対して QoS ポリシーは適用または削除されません。そのような接続の QoS ポリシーを適用または削除するには、接続をクリア（つまりドロップ）して再確立する必要があります。

**例**

次に、出力方向の **police** コマンドの例を示します。このコマンドは、適合レートを 100,000 ビット / 秒、バースト値を 20,000 バイトに設定し、バースト レートを超えたトラフィックはドロップされるように指定します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class-map firstclass
hostname(config-cmap)# class localclass
hostname(config-pmap-c)# police output 100000 20000 exceed-action drop
hostname(config-cmap-c)# class class-default
hostname(config-pmap-c)#
```

次に、内部 Web サーバを宛先とするトラフィックにレート制限を実行する例を示します。

```
hostname# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
```

```
hostname# class-map http_traffic
hostname(config-cmap)# match access-list http_traffic
hostname(config-cmap)# policy-map outside_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# police input 56000
hostname(config-pmap-c)# service-policy outside_policy interface outside
hostname(config)#
```

## 関連コマンド

| | |
|---|---|
| **class** | トラフィックの分類に使用するクラス マップを指定します。 |
| **clear configure policy-map** | すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# policy

CRL の取得元を指定するには、ca-crl コンフィギュレーション モードで **policy** コマンドを使用します。

**policy** {**static | cdp | both**}

## 構文の説明

| | |
|---|---|
| **both** | CRL 配布ポイントを使用した CRL の取得に失敗した場合は、スタティック CDP を最大 5 つ使用して再試行します。 |
| **cdp** | チェック対象の証明書内に埋め込まれている CDP 拡張を使用します。この場合、セキュリティ アプライアンスは検証対象の証明書の CDP 拡張から最大 5 つの CRL 配布ポイントを取得します。さらに必要に応じて、設定されたデフォルト値を使用して情報を増強します。セキュリティ アプライアンスがプライマリ CDP を使用して CRL を取得するのに失敗した場合は、リストで次に使用可能な CDP を使用して再試行します。これは、セキュリティ アプライアンスが CRL を取得するかリストの最後に到達するまで、繰り返されます。 |
| **static** | 最大で 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドを使用して LDAP または HTTP URL も指定します。 |

## デフォルト

デフォルトの設定は **cdp** です。

## コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| CRL コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 例

次に、ca-crl コンフィギュレーション モードを開始し、チェック対象の証明書内にある CRL 配布ポイント拡張を使用して CRL 取得を行うように設定し、失敗した場合はスタティック CDP を使用する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **crl configure** | ca-crl コンフィギュレーション モードを開始します。 |
| **crypto ca trustpoint** | トラストポイント コンフィギュレーション モードを開始します。 |
| **url** | CRL 取得用のスタティック URL のリストを作成および維持します。 |

# policy-map

モジュラ ポリシー フレームワーク を使用する場合、レイヤ 3/4 のクラスマップ（**class-map** または **class-map type management** コマンド）を使用してトラフィックにアクションを割り当てるには、グローバル コンフィギュレーション モードで **policy-map** コマンド（**type** キーワードの指定なし）を使用します。レイヤ 3/4 ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

**policy-map** *name*

**no policy-map** *name*

## 構文の説明

| | |
|---|---|
| *name* | このポリシー マップの名前を最大 40 文字で指定します。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

ポリシー マップの最大数は 64 です。レイヤ 3/4 ポリシー マップ内にある複数のレイヤ 3/4 クラス マップを特定でき（**class** コマンドを参照）、1 つ以上の機能タイプから各クラス マップへ複数のアクションを割り当てることができます。

パケットは、各機能タイプのポリシー マップで、1 つのクラス マップにだけ一致します。パケットが機能タイプのクラス マップと一致する場合、セキュリティ アプライアンスはその機能タイプについて後続のクラス マップと照合しません。ただし、パケットが別の機能タイプについて後続のクラス マップと一致する場合、セキュリティ アプライアンスでは後続のクラス マップについてもアクションを適

用します。たとえば、パケットが接続制限についてのクラス マップと一致し、さらにアプリケーション インスペクションについてのクラス マップとも一致する場合は、両方のクラス マップ アクションが適用されます。パケットがアプリケーション インスペクションについてのクラス マップと一致し、さらにアプリケーション インスペクションについての別のクラス マップとも一致する場合、2 番めのクラス マップ アクションは適用されません。

アクションは、機能に応じて双方向または単方向にトラフィックに適用されます。双方向に適用される機能の場合、トラフィックが両方向のクラス マップと一致した場合に、ポリシー マップを適用するインターフェイスを出入りするすべてのトラフィックが影響を受けます。

**（注）** グローバル ポリシーを使用する場合は、すべての機能が単方向です。単一インターフェイスに適用する場合に通常双方向の機能は、グローバルに適用される場合、各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは両方向に適用され、この場合の双方向は冗長になります。

QoS のように単方向に適用される機能では、ポリシー マップの適用先インターフェイスから出るトラフィックのみが影響を受けます。各機能の方向については、表 22-1 を参照してください。

**表 22-1　機能の方向**

| 機能 | 単一インターフェイスでの方向 | グローバルでの方向 |
|---|---|---|
| TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化 | 双方向 | 入力 |
| CSC | 双方向 | 入力 |
| アプリケーション インスペクション | 双方向 | 入力 |
| IPS | 双方向 | 入力 |
| QoS ポリシング | Egress | Egress |
| QoS プライオリティ キュー | Egress | Egress |

ポリシー マップの各種のアクションが実行される順序は、ポリシー マップ中に出現する順序とは無関係です。アクションは次の順序で実行されます。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化

**（注）** セキュリティ アプライアンスがプロキシ サービス（AAA や CSC など）を実行したり、TCP ペイロード（FTP インスペクション）を変更したりするときは、TCP ノーマライザはデュアル モードで動作します。その場合、サービスを変更するプロキシやペイロードの前後で適用されます。

- CSC
- アプリケーション インスペクション
- IPS
- QoS ポリシング
- QoS プライオリティ キュー

インターフェイスあたりに割り当てられるポリシー マップは 1 つだけですが、同じポリシー マップを複数のインターフェイスに割り当てることができます。

コンフィギュレーションには、デフォルト グローバル ポリシーでセキュリティ アプライアンスが使用する、デフォルトのレイヤ 3/4 ポリシー マップが含まれています。これは **global_policy** と呼ばれ、デフォルトのインスペクション トラフィックでインスペクションを実行します。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。

デフォルトのポリシー マップ コンフィギュレーションには、次のコマンドが含まれます。

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

## 例

接続ポリシーの **policy-map** コマンドの例を次に示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
```

```
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、セキュリティ アプライアンスはこの照合を行いません。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップのクラス マップ名を指定します。 |
| **clear configure policy-map** | すべてのポリシー マップ コンフィギュレーションを削除します。ポリシー マップが **service-policy** コマンドで使用されている場合、そのポリシー マップは削除されません。 |
| **class-map** | トラフィック クラス マップを定義します。 |
| **service-policy** | ポリシー マップをインターフェイスに割り当てるか、またはすべてのインターフェイスにグローバルに割り当てます。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# policy-map type inspect

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map type inspect** コマンドを使用して、アプリケーション トラフィック検査のための特別なアクションを定義します。インスペクション ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

**policy-map type inspect** *application policy_map_name*

**no policy-map** [**type inspect** *application*] *policy_map_name*

## 構文の説明

| | |
|---|---|
| *application* | 対象とするアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。<br>• **dcerpc**<br>• **dns**<br>• **esmtp**<br>• **ftp**<br>• **gtp**<br>• **h323**<br>• **http**<br>• **im**<br>• **mgcp**<br>• **netbios**<br>• **radius-accounting**<br>• **rtsp**<br>• **sip**<br>• **skinny**<br>• **snmp** |
| *policy_map_name* | このポリシー マップの名前を最大 40 文字で指定します。「_internal」または「_default」で始まる名前は予約されており、使用できません。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。 |

## デフォルト

デフォルトの動作や値はありません。

**コマンド モード**　次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | — |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 7.2(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**　モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 のポリシー マップ（**policy-map** コマンド）で、**inspect** コマンドを使用してインスペクション エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシー マップで定義されているアクションを、オプションでイネーブルにすることもできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

インスペクション ポリシー マップは、ポリシー マップ コンフィギュレーション モードで入力するコマンドのうち、次の 1 つ以上のコマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。

- **match** コマンド：**match** コマンドをインスペクション ポリシー マップで直接定義して、アプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合できます。次に、一致コンフィギュレーション モードで **drop**、**reset**、**log** などのアクションをイネーブルにします。**match** コマンドを使用できるかどうかは、アプリケーションによって異なります。
- **class** コマンド：このコマンドは、ポリシー マップ内のインスペクション クラス マップを特定します（インスペクション クラス マップの作成については、**class-map type inspect** コマンドを参照してください）。インスペクション クラス マップには、**match** コマンドが含まれます。このコマンドは、ポリシー マップ内のアクションをイネーブルにするアプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合します。クラス マップを作成することと、インスペクション ポリシー マップ内で **match** コマンドを直接使用することの違いは、複数の照合結果をグループ化できることと、クラス マップを再使用できることです。
- **parameters** コマンド：パラメータは、インスペクション エンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

ポリシー マップには、複数の **class** コマンドまたは **match** コマンドを指定できます。

一部の **match** コマンドでは、パケット内のテキストと一致させるために正規表現を指定できます。**regex** コマンドおよび **class-map type regex** コマンド（複数の正規表現をグループ化）を参照してください。

デフォルトのインスペクション ポリシー マップ コンフィギュレーションには、次のコマンドが組み込まれています。このコンフィギュレーションでは、DNS パケットの最大メッセージ長を 512 バイトに設定しています。

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

1 つのパケットが複数の異なる **match** コマンドまたは **class** コマンドと一致する場合、セキュリティ アプライアンス がアクションを適用する順序は、ポリシー マップにアクションが追加された順序ではなく、セキュリティ アプライアンスの内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
hostname(config-pmap)# match request header host length gt 100
hostname(config-pmap-c)# reset
hostname(config-pmap-c)# match request method get
hostname(config-pmap-c)# log
```

アクションがパケットをドロップすると、それ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドが一致することはありません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます 同じ **match** コマンドに対して **reset**（または **drop-connection** など）と **log** アクションの両方を設定できます。この場合、特定の match でリセットされるまでパケットはログに記録されます。

パケットが、同じ複数の **match** コマンドまたは **class** コマンドと照合される場合は、ポリシー マップ内のそれらのコマンドの順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが行われ、ログには記録されません。

```
hostname(config-pmap)# match request header length gt 100
hostname(config-pmap-c)# log
hostname(config-pmap-c)# match request header length gt 1000
hostname(config-pmap-c)# reset
```

クラス マップは、そのクラス マップ内で重要度が最低の **match** コマンド（重要度は、内部ルールに基づきます）に基づいて、別のクラス マップまたは **match** コマンドと同じタイプであると判断されます。クラス マップに、別のクラス マップと同じタイプの重要度が最低の **match** コマンドがある場合、それらのクラス マップはポリシー マップに追加された順序で照合されます。クラス マップごとに最低重要度のコマンドが異なる場合は、最高重要度の **match** コマンドを持つクラス マップが最初に照合されます。

## 例

次の例では、HTTP インスペクション ポリシー マップとその関連クラス マップを示します。このポリシー マップは、サービス ポリシーがイネーブルにするレイヤ 3/4 ポリシー マップによってアクティブになります。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
```

```
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test (a Layer 3/4 class map not shown)
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy inbound_policy interface outside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップのクラス マップ名を指定します。 |
| **class-map type inspect** | アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。 |
| **parameters** | インスペクション ポリシー マップのパラメータ コンフィギュレーション モードを開始します。 |
| **policy-map** | レイヤ 3/4 のポリシー マップを作成します。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# policy-server-secret

SiteMinder SSO サーバへの認証要求を暗号化するために使用する秘密キーを設定するには、webvpn sso siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用します。秘密キーを削除するには、このコマンドの **no** 形式を使用します。

**policy-server-secret** *secret-key*

**no policy-server-secret**

**（注）** このコマンドは、SiteMinder SSO 認証で必要です。

## 構文の説明

| | |
|---|---|
| *secret-key* | 認証通信を暗号化するために秘密キーとして使用されるストリング。文字の最小数や最大数の制限はありません。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| config-webvpn-sso-siteminder コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.1(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

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。まず **sso-server** コマンドを使用して SSO サーバを作成します。SiteMinder SSO サーバの場合、**policy-server-secret** コマンドによってセキュリティ アプライアンスと SSO サーバの間の認証通信を保護します。

コマンド引数 *secret-key* は、パスワードと同様に作成、保存、および設定が可能です。このコマンド引数は、**policy-server-secret** コマンドを使用してセキュリティ アプライアンスで設定され、Cisco Java プラグイン認証方式を使用して SiteMinder Policy Server で設定されます。

このコマンドは、SiteMinder-type の SSO サーバにのみ適用されます。

## 例

次に、config-webvpn-sso-siteminder モードで、引数としてランダムなストリングを使用して、SiteMinder SSO サーバ認証通信の秘密キーを作成する例を示します。

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
```

```
hostname(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
hostname(config-webvpn-sso-siteminder)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **max-retry-attempts** | セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数を設定します。 |
| **request-timeout** | SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。 |
| **show webvpn sso-server** | セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。 |
| **sso-server** | シングル サインオン サーバを作成します。 |
| **test sso-server** | テスト認証要求で SSO サーバをテストします。 |
| **web-agent-url** | セキュリティ アプライアンスが SiteMinder SSO 認証を要求する SSO サーバの URL を指定します。 |

# polltime interface

Active/Active フェールオーバー コンフィギュレーションのデータ インターフェイス ポーリング タイムおよびホールド タイムを指定するには、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**polltime interface** [**msec**] *time* [**holdtime** *time*]

**no polltime interface** [**msec**] *time* [**holdtime** *time*]

## 構文の説明

| | |
|---|---|
| **holdtime** *time* | （任意）データ インターフェイスがピア インターフェイスから hello メッセージを受信する必要のある時間を設定します。この時間の経過後、ピア インターフェイスが障害状態であると宣言されます。有効な値は 5 ～ 75 秒です。 |
| **interface** *time* | データ インターフェイスのポーリング期間を指定します。有効な値は、3 ～ 15 秒です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。 |
| **msec** | （任意）指定する時間がミリ秒単位であることを指定します。 |

## デフォルト

ポーリングの *time* は 5 秒です。

**holdtime** *time* は、ポーリングの *time* の 5 倍です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| フェールオーバー グループ コンフィギュレーション | • | • | — | — | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(1) | このコマンドが導入されました。 |
| 7.2(1) | このコマンドは、任意の **holdtime** *time* 値とポーリング タイムをミリ秒で指定する機能を含めるように変更されました。 |

## 使用上のガイドライン

指定されたフェールオーバー グループと関連付けられたインターフェイスから hello パケットが送信される頻度を変更するには、**polltime interface** コマンドを使用します。このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。Active/Standby フェールオーバー コンフィギュレーションで **failover polltime interface** コマンドを使用します。

ポーリング タイムの 5 倍よりも短い **holdtime** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。ホールド タイムの半分が経過したときに、インターフェイスで hello パケットが受信されていない場合は、インターフェイスのテストが開始されます。

**failover polltime unit** コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

**（注）** CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスをパススルーする場合は、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

## 例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。フェールオーバー グループ 1 のデータ インターフェイスのインターフェイス ポーリング時間を 500 ミリ秒に設定し、保持時間を 5 秒に設定します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface msec 500 holdtime 5
hostname(config-fover-group)# exit
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **failover group** | Active/Active フェールオーバーのためのフェールオーバー グループを定義します。 |
| **failover polltime** | 装置のフェールオーバー ポーリング期間とホールド タイムを指定します。 |
| **failover polltime interface** | Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間およびホールド タイムを指定します。 |

# pop3s

POP3S コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **pop3s** コマンドを使用します。POP3S コマンド モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

POP3 は、インターネット サーバが電子メールを受信して保持するために使用するクライアント/サーバ プロトコルです。ユーザ（またはクライアント電子メール レシーバ）は、定期的にメールボックスをチェックして、メールがある場合はそれをダウンロードします。この標準プロトコルは、ほとんどの著名な電子メール製品に組み込まれています。POP3S を使用すると、SSL 接続で電子メールを受信できます。

**pop3s**

**no pop3**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | — | — | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 例

次に、POP3S コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure pop3s** | POP3S コンフィギュレーションを削除します。 |
| **show running-config pop3s** | POP3S の実行コンフィギュレーションを表示します。 |

# port

電子メール プロキシで受信に使用されるポートを指定するには、適切な電子メール プロキシ コマンド モードで **port** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**port** {*portnum*}

**no port**

## 構文の説明

| | |
|---|---|
| portnum | 電子メール プロキシで使用するポート。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。 |

## デフォルト

電子メール プロキシのデフォルト ポートは次のとおりです。

| 電子メール プロキシ | デフォルト ポート |
|---|---|
| IMAP4S | 993 |
| POP3S | 995 |
| SMTPS | 988 |

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| pop3s | • | — | • | — | — |
| Imap4s | • | — | • | — | — |
| Smtps | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

## 例

次に、IMAP4S 電子メール プロキシ用にポート 1066 を設定する例を示します。

```
hostname(config)# imap4s
hostname(config-imap4s)# port 1066
```

# port-forward

クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートからアクセスできるアプリケーション セットを設定するには、webvpn コンフィギュレーション モードで **port-forward** コマンドを使用します。

**port-forward** {*list_name local_port remote_server remote_port description*}

複数アプリケーションへのアクセスを設定するには、アプリケーションごとに同じ *list_name* を 1 回ずつ、複数回指定してこのコマンドを使用します。

リストから設定済みアプリケーションを削除するには、**no port-forward** *list_name local_port* コマンドを使用します（*remote_server* および *remote_port* パラメータを指定する必要はありません）。

**no port-forward** *listname localport*

設定済みのリスト全体を削除するには、**no port-forward** *list_name* コマンドを使用します。

**no port-forward** *list_name*

## 構文の説明

| | |
|---|---|
| *description* | エンド ユーザのポート フォワーディング Java アプレット画面に表示されるアプリケーション名または短い説明を指定します。最大 64 文字です。 |
| *list_name* | クライアントレス SSL VPN セッションのユーザがアクセスできる一連のアプリケーション（転送先 TCP ポート）をグループ化します。最大 64 文字です。 |
| *local_port* | アプリケーションの TCP トラフィックを受信するローカル ポートを指定します。ローカル ポート番号は *list_name* あたり 1 回のみ使用できます。1 ～ 65535 の範囲のポート番号を入力します。既存サービスとの競合を避けるために、1024 よりも大きいポート番号を使用します。 |
| *remote_port* | リモート サーバでこのアプリケーション用に接続するポートを指定します。これは、アプリケーションで使用する実際のポートです。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。 |
| *remote_server* | アプリケーションのリモート サーバの DNS 名または IP アドレスを指定します。これには DNS 名を使用することを推奨します。IP アドレスを入力する場合は、IPv4 形式か IPv6 形式で入力できます。 |

## デフォルト

デフォルトのポート フォワーディング リストはありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| webvpn コンフィギュレーション モード | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |
| 8.0(2) | コマンド モードが webvpn に変更されました。 |

## 使用上のガイドライン

セキュリティ アプライアンスは Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。クライアントレス SSL VPN セッションを介してアプリケーション アクセスを提供する、ポート フォワーディングとスマート トンネル機能のいずれも、MAPI をサポートしていません。MAPI プロトコルを使用した Microsoft Outlook Exchange 通信では、リモート ユーザが AnyConnect を使用する必要があります。

## 例

次の表に、サンプル アプリケーションで使用する値を示します。

| アプリケーション | Local Port | サーバ DNS 名 | Remote Port | 説明 |
|---|---|---|---|---|
| IMAP4S 電子メール | 20143 | IMAP4Sserver | 143 | メール取得 |
| SMTPS 電子メール | 20025 | SMTPSserver | 25 | メール送信 |
| DDTS over SSH | 20022 | DDTSserver | 22 | DDTS over SSH |
| Telnet | 20023 | Telnetserver | 23 | Telnet |

次に、これらのアプリケーションへのアクセスを提供する *SalesGroupPorts* という名前のポート フォワーディング リストを作成する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config-webvpn)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config-webvpn)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config-webvpn)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **port-forward auto-start** | このコマンドはグループ ポリシー webvpn またはユーザ名 webvpn モードで入力します。ユーザがクライアントレス SSL VPN セッションにログインするときに、ポート フォワーディングを自動的に開始して、指定したポート フォワーディング リストを割り当てます。 |
| **port-forward enable** | このコマンドはグループ ポリシー webvpn またはユーザ名 webvpn モードで入力します。ユーザがログインするときに、指定したポート フォワーディング リストを割り当てますが、ポート フォワーディングはユーザが手動で開始する必要があります。開始するには、クライアントレス SSL VPN ポータル ページで [Application Access] > [Start Applications] ボタンを使用します。 |
| **port-forward disable** | このコマンドはグループ ポリシー webvpn またはユーザ名 webvpn モードで入力します。ポート フォワーディングをオフにします。 |

# port-forward-name

特定のユーザ ポリシーやグループ ポリシーのエンド ユーザに対して TCP ポート フォワーディングを特定する表示名を設定するには、webvpn モードで **port-forward-name** コマンドを使用します。このモードは、グループ ポリシー モードまたはユーザ名モードから開始します。表示名（**port-forward-name none** コマンドを使用して作成されたヌル値を含む）を削除するには、このコマンドの no 形式を使用します。**no** オプションを使用するとデフォルト名「Application Access」に戻ります。表示名を使用しないようにするには、**port-forward none** コマンドを使用します。

**port-forward-name** {**value** *name* | **none**}

**no port-forward-name**

## 構文の説明

| | |
|---|---|
| **none** | 表示名がないことを指定します。ヌル値を設定して、表示名を拒否します。値は継承しません。 |
| **value** *name* | エンド ユーザにポート フォワーディングを説明します。最大 255 文字です。 |

## デフォルト

デフォルト名は「Application Access」です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| webvpn | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 例

次に、FirstGroup という名前のグループ ポリシーに対して「Remote Access TCP Applications」という名前を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **webvpn** | グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。 |
| **webvpn** | グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。 |

# port-object

サービス オブジェクト グループにポート オブジェクトを追加するには、サービス コンフィギュレーション モードで **port-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

**port-object eq** *service*

**no port-object eq** *service*

**port-object range** *begin_service end_service*

**no port-object range** *begin_service end_service*

## 構文の説明

| | |
|---|---|
| begin_service | サービスの範囲の開始値である、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 とする必要があります。 |
| end_service | サービスの範囲の終了値である TCP または UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 とする必要があります。 |
| **eq** service | サービス オブジェクトの TCP または UDP ポートの 10 進数または名前を指定します。 |
| **range** | ポートの範囲（両端を含む）を指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| サービス コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

**port-object** コマンドは、**object-group** コマンドとともに使用して、サービス コンフィギュレーション モードで特定サービス（ポート）またはサービス（ポート）の範囲であるオブジェクトを定義します。

TCP または UDP サービスの名前を指定する場合は、サポートされる TCP や UDP のいずれかの名前で、オブジェクト グループのプロトコル タイプと整合性を持つものである必要があります。たとえば、プロトコル タイプが tcp、udp、および tcp-udp の場合、名前はそれぞれ有効な TCP サービス名、有効な UDP サービス名、または有効な TCP および UDP サービス名である必要があります。

番号を指定した場合、オブジェクトが表示されるときに、プロトコル タイプに基づいて、その番号が対応する名前（存在する場合）に変換されます。

次のサービス名がサポートされています。

| TCP | UDP | TCP および UDP |
|---|---|---|
| bgp | biff | discard |
| chargen | bootpc | domain |
| cmd | bootps | echo |
| daytime | dnsix | pim-auto-rp |
| exec | nameserver | sunrpc |
| finger | mobile-ip | syslog |
| ftp | netbios-ns | tacacs |
| ftp-data | netbios-dgm | talk |
| gopher | ntp | |
| ident | rip | |
| irc | snmp | |
| h323 | snmptrap | |
| hostname | tftp | |
| http | time | |
| klogin | who | |
| kshell | xdmcp | |
| login | isakmp | |
| lpd | | |
| nntp | | |
| pop2 | | |
| pop3 | | |
| smtp | | |
| sqlnet | | |
| telnet | | |
| uucp | | |
| whois | | |
| www | | |

**例**

次に、新規ポート（サービス）オブジェクト グループを作成するために、サービス コンフィギュレーション モードで **port-object** コマンドを使用する例を示します。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
hostname(config-service)# port-object eq snmp
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure object-group** | すべての **object-group** コマンドをコンフィギュレーションから削除します。 |
| **group-object** | ネットワーク オブジェクト グループを追加します。 |
| **network-object** | ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。 |
| **object-group** | コンフィギュレーションを最適化するためのオブジェクト グループを定義します。 |
| **show running-config object-group** | 現在のオブジェクト グループを表示します。 |

# post-max-size

オブジェクトのポストが許可される最大サイズを指定するには、グループ ポリシー webvpn コンフィギュレーション モードで **post-max-size** コマンドを使用します。このオブジェクトをコンフィギュレーションから削除するには、このコマンドの **no** バージョンを使用します。

**post-max-size** <*size*>

**no post-max-size**

## 構文の説明

| | |
|---|---|
| *size* | ポストするオブジェクトに許可される最大サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。 |

## デフォルト

デフォルトのサイズは 2147483647 です。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グループ ポリシー webvpn コンフィギュレーション モード | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

サイズを 0 に設定すると、オブジェクトのポストが実質的に禁止されます。

## 例

次に、ポストするオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
hostname(config)# group-policy test attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# post-max-size 1500
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **download-max-size** | ダウンロードするオブジェクトの最大サイズを指定します。 |
| **upload-max-size** | アップロードするオブジェクトの最大サイズを指定します。 |

| コマンド | 説明 |
|---|---|
| **webvpn** | グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。 |
| **webvpn** | グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。 |

# pppoe client route distance

PPPoE を介して学習したルートのアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

**pppoe client route distance** *distance*

**no pppoe client route distance** *distance*

## 構文の説明

| | |
|---|---|
| *distance* | PPPoE を介して学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。 |

## デフォルト

PPPoE を介して学習したルートには、デフォルトで 1 のアドミニストレーティブ ディスタンスが割り当てられます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

ルートが PPPoE から学習されたときにのみ、**pppoe client route distance** コマンドがチェックされます。ルートが PPPoE から学習された後で **pppoe client route distance** コマンドを入力しても、指定したアドミニストレーティブ ディスタンスは既存の学習済みルートに影響しません。指定したアドミニストレーティブ ディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE によりルートを取得するには、**ip address pppoe** コマンドに **setroute** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートのプライオリティを示す必要があります。複数のインターフェイスでの PPPoE クライアントのイネーブル化は、オブジェクト トラッキングでのみサポートされています。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

## 例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ip address pppoe** | PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。 |
| **ppoe client secondary** | セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。 |
| **pppoe client route track** | PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。 |
| **sla monitor** | SLA モニタリング動作を定義します。 |
| **track rtr** | SLA をポーリングするためのトラッキング エントリを作成します。 |

# pppoe client route track

PPPoE クライアントを設定して、追加されたルートを指定されたトラッキング済みオブジェクト番号に関連付けるには、インターフェイス コンフィギュレーション モードで **pppoe client route track** コマンドを使用します。PPPoE ルート トラッキングを削除するには、このコマンドの **no** 形式を使用します。

**pppoe client route track** *number*

**no pppoe client route track**

## 構文の説明

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

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

ルートが PPPoE から学習されたときにのみ、**pppoe client route track** コマンドがチェックされます。ルートが PPPoE から学習された後に **pppoe client route track** コマンドを入力した場合、既存の学習されたルートはトラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE によりルートを取得するには、**ip address pppoe** コマンドに **setroute** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートのプライオリティを示す必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

## 例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ip address pppoe** | PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。 |
| **ppoe client secondary** | セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。 |
| **pppoe client route distance** | PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。 |
| **sla monitor** | SLA モニタリング動作を定義します。 |
| **track rtr** | SLA をポーリングするためのトラッキング エントリを作成します。 |

# pppoe client secondary

PPPoE クライアントをトラッキング済みオブジェクトのクライアントとして登録し、トラッキング状態に基づいて起動または終了するように設定するには、インターフェイス コンフィギュレーション モードで **pppoe client secondary** コマンドを使用します。クライアントの登録を削除するには、このコマンドの **no** 形式を使用します。

**pppoe client secondary track** *number*

**no pppoe client secondary track**

## 構文の説明

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

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| インターフェイス コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

PPPoE セッションが開始されたときにのみ、**pppoe client secondary** コマンドがチェックされます。ルートが PPPoE から学習された後に **pppoe client route track** コマンドを入力した場合､既存の学習されたルートはトラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE によりルートを取得するには、**ip address pppoe** コマンドに **setroute** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートのプライオリティを示す必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

## 例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニタされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **ip address pppoe** | PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。 |
| **ppoe client secondary** | セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。 |
| **pppoe client route distance** | PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。 |
| **pppoe client route track** | PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。 |
| **sla monitor** | SLA モニタリング動作を定義します。 |

# pre-fill-username

認証と認可で使用するクライアント証明書からユーザ名を抽出できるようにするには、トンネル グループ webvpn 属性モードで **pre-fill-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

**pre-fill-username** {**ssl-client** | **clientless**}

**no pre-fill-username**

## 構文の説明

| | |
|---|---|
| **ssl-client** | この機能を AnyConnect VPN クライアント接続でイネーブルにします。 |
| **clientless** | この機能をクライアントレス接続でイネーブルにします。 |

## デフォルト

デフォルトの値や動作はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ webvpn 属性コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | このコマンドが導入されました。 |

## 使用上のガイドライン

**pre-fill-username** コマンドを使用すると、ユーザ名 / パスワードによる認証と認可のユーザ名として、**username-from-certificate** コマンドで指定した証明書のフィールドから抽出したユーザ名を使用できます。証明書機能からこの事前充填ユーザ名を使用するには、両方のコマンドを設定する必要があります。

この機能をイネーブルにするには、トンネル グループ一般属性モードで **usesrname-from-certificate** コマンドを設定する必要もあります。

**（注）** リリース 8.0.4 では、ユーザ名は事前に入力されません。ユーザ名フィールド内の送信されたデータは無視されます。

## 例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループを作成し、SSL VPN クライアントの認証または認可クエリーの名前をデジタル証明書から取得する必要があることを指定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp webvpn-attributes
```

```
hostname(config-tunnel-webvpn)# pre-fill-username ssl-client
hostname(config-tunnel-webvpn)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **pre-fill-username** | 事前入力ユーザ名機能をイネーブルにします。 |
| **show running-config tunnel-group** | 指定されたトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group general-attributes** | 名前付きのトンネル グループの一般属性を指定します。 |

# preempt

ユニットのプライオリティが高い場合にそのユニットをブート時にアクティブにするには、フェールオーバー グループ コンフィギュレーション モードで **preempt** コマンドを使用します。プリエンプションを削除するには、このコマンドの **no** 形式を使用します。

**preempt** [*delay*]

**no preempt** [*delay*]

## 構文の説明

| | |
|---|---|
| *seconds* | ピアがプリエンプション処理されるまでの待機時間（秒数）。有効な値は、1 ～ 1200 秒です。 |

## デフォルト

デフォルトでは遅延はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| フェールオーバー グループ コンフィギュレーション | • | • | — | — | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

プライマリまたはセカンダリのプライオリティをフェールオーバー グループに割り当てると、両方のユニットが（ユニットのポーリング期間内で）同時にブートしたときに、フェールオーバー グループがどのユニット上でアクティブになるかが指定されます。しかし、ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバー グループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバー グループが自動的にアクティブになります。

**（注）** ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

## 例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どちらのフェールオーバー グループも **preempt** コマンドで待機時間が 100 秒に設定されているため、グループは、ユニットが使用可能になった 100 秒後に自動的にその優先ユニットでアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **failover group** | Active/Active フェールオーバーのためのフェールオーバー グループを定義します。 |
| **primary** | 設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、プライマリ ユニットを指定します。 |
| **secondary** | 設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、セカンダリ ユニットを指定します。 |

# prefix-list

ABR のタイプ 3 LSA フィルタリングのプレフィックス リストにエントリを作成するには、グローバル コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィックス リストのエントリを削除するには、このコマンドの **no** 形式を使用します。

**prefix-list** *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

**no prefix-list** *prefix-list-name* [**seq** *seq_num*] {**permit | deny**} *network/len* [**ge** *min_value*] [**le** *max_value*]

## 構文の説明

| | |
|---|---|
| / | *network* 値と *len* 値との間に必要な区切り文字。 |
| **deny** | 一致した条件へのアクセスを拒否します。 |
| **ge** *min_value* | （任意）照会されるプレフィックスの最小の長さを指定します。*min_value* 引数の値は、*len* 引数の値よりも大きく、*max_value* 引数が存在する場合はそれ以下である必要があります。 |
| **le** *max_value* | （任意）照会されるプレフィックスの最大の長さを指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合はその値以上、*min_value* 引数が存在しない場合は *len* 引数よりも大きい値にする必要があります。 |
| *len* | ネットワーク マスクの長さ。有効な値は、0 ～ 32 です。 |
| *network* | ネットワーク アドレス。 |
| **permit** | 一致した条件へのアクセスを許可します。 |
| *prefix-list-name* | プレフィックス リストの名前。プレフィックス リスト名にスペースを含めることはできません。 |
| **seq** *seq_num* | （任意）作成するプレフィックス リストに指定されたシーケンス番号を適用します。 |

## デフォルト

シーケンス番号を指定しない場合、プレフィックス リストの先頭エントリにはシーケンス番号 5 が割り当てられ、その後のエントリのシーケンス番号は 5 ずつ増えていきます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

**prefix-list** コマンドは、ABR のタイプ 3 LSA フィルタリング コマンドです。ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されると、指定したプレフィックスのみがエリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。セキュリティ アプライアンスでは、プレフィックス リストの先頭、つまりシーケンス番号が最も小さいエントリから検索を開始します。一致が見つかると、セキュリティ アプライアンスはリストの残りの部分を調べません。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

デフォルトでは、シーケンス番号は自動的に生成されます。自動生成されるシーケンス番号を抑制するには、**no prefix-list sequence-number** コマンドを使用します。シーケンス番号は、5 ずつ増分されます。プレフィックス リストで生成される最初のシーケンス番号は 5 です。そのリストの次のエントリにはシーケンス番号 10 が設定され、以降も同様に設定されます。あるエントリに値を指定し、その後のエントリに値を指定しない場合、生成されるシーケンス番号は指定された値から 5 ずつ増分されます。たとえば、プレフィックス リストの最初のエントリのシーケンス番号を 3 と指定し、その後シーケンス番号を指定しないで 2 つのエントリを追加した場合、これら 2 つエントリに対して自動的に生成されるシーケンス番号は、8 および 13 となります。

**ge** キーワードおよび **le** キーワードを使用して、*network*/*len* 引数よりも具体的なプレフィックスに対して一致するプレフィックス長の範囲を指定できます。**ge** キーワードも **le** キーワードも指定されていないときは、完全一致であると見なされます。**ge** キーワードのみが指定されている場合の範囲は、*min_value* ～ 32 です。**le** キーワードのみが指定されている場合の範囲は、*len* ～ *max_value* です。

*min_value* 引数および *max_value* 引数の値は、次の条件を満たす必要があります。

*len* < *min_value* <= *max_value* <= 32

プレフィックス リストから特定のエントリを削除するには、このコマンドの **no** 形式を使用します。プレフィックス リストを削除するには、**clear configure prefix-list** コマンドを使用します。**clear configure prefix-list** コマンドを使用すると、関連する **prefix-list description** コマンドがある場合は、それもコンフィギュレーションから削除されます。

## 例

次に、デフォルト ルート 0.0.0.0/0 を拒否する例を示します。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

次に、プレフィックス 10.0.0.0/8 を許可する例を示します。

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

次に、プレフィックス 192/8 のルートで最大 24 ビットのマスク長を許可する例を示します。

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

次に、プレフィックス 192/8 のルートで 25 ビットよりも大きいマスク長を拒否する例を示します。

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

次に、すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する例を示します。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次に、すべてのアドレス空間で 25 ビットよりも大きいマスク長を拒否する例を示します。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

次に、プレフィックス 10/8 のすべてのルートを拒否する例を示します。

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

次に、プレフィックス 192.168.1/24 のルートで 25 ビットよりも大きいすべてのマスクを拒否する例を示します。

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

次に、プレフィックス 0/0 のすべてのルートを許可する例を示します。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure prefix-list** | **prefix-list** コマンドを実行コンフィギュレーションから削除します。 |
| **prefix-list description** | プレフィックス リストの説明を入力できます。 |
| **prefix-list sequence-number** | プレフィックス リストのシーケンス番号付けをイネーブルにします。 |
| **show running-config prefix-list** | 実行コンフィギュレーション内の **prefix-list** コマンドを表示します。 |

# prefix-list description

プレフィックス リストに説明を追加するには、グローバル コンフィギュレーション モードで **prefix-list description** コマンドを使用します。プレフィックス リストの説明を削除するには、このコマンドの **no** 形式を使用します。

**prefix-list** *prefix-list-name* **description** *text*

**no prefix-list** *prefix-list-name* **description** [*text*]

## 構文の説明

| | |
|---|---|
| *prefix-list-name* | プレフィックス リストの名前。 |
| *text* | プレフィックス リストの説明テキスト。最大 80 文字を入力できます。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

**prefix-list** コマンドおよび **prefix-list description** コマンドは、特定のプレフィックス リスト名に対して、任意の順序で入力できます。プレフィックス リストの説明を入力する前に、プレフィックス リストを作成する必要はありません。**prefix-list description** コマンドは、コマンドを入力する順序に関係なく、コンフィギュレーションで関連するプレフィックス リストの前の行に必ず記述されます。

すでに説明の設定されたプレフィックス リスト エントリに対して **prefix-list description** コマンドを入力した場合、新しい説明によって元の説明が置き換えられます。

このコマンドの **no** 形式を使用するときは、テキスト説明を入力する必要はありません。

## 例

次に、MyPrefixList という名前のプレフィックス リストの説明を追加する例を示します。**show running-config prefix-list** コマンドは、プレフィックス リストの説明が実行コンフィギュレーションに追加された場合でも、プレフィックス リスト自体は設定されていないことを示します。

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
!
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure prefix-list** | **prefix-list** コマンドを実行コンフィギュレーションから削除します。 |
| **prefix-list** | ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。 |
| **show running-config prefix-list** | 実行コンフィギュレーション内の **prefix-list** コマンドを表示します。 |

# prefix-list sequence-number

プレフィックス リストのシーケンス番号付けをイネーブルにするには、グローバル コンフィギュレーション モードで **prefix-list sequence-number** コマンドを使用します。プレフィックス リストのシーケンス番号付けをディセーブルにするには、このコマンドの **no** 形式を使用します。

**prefix-list sequence-number**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

プレフィックス リストのシーケンス番号付けは、デフォルトでイネーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。このコマンドの **no** 形式がコンフィギュレーション内にある場合、シーケンス番号（手動設定したものを含む）はコンフィギュレーション内の **prefix-list** コマンドから削除されます。プレフィックス リストの新しいエントリにシーケンス番号は割り当てられません。

プレフィックス リストのシーケンス番号付けがイネーブルの場合、デフォルトの番号付け方式（5 で始まり、番号が 5 ずつ増分される）を使用して、プレフィックス リストのすべてのエントリにシーケンス番号が割り当てられます。番号付けがディセーブルになる前に、シーケンス番号がプレフィックス リストのエントリに手動で割り当てられた場合、手動で割り当てられた番号が復元されます。自動番号付けがディセーブルのときに手動で割り当てたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間、これらのシーケンス番号は表示されません。

## 例

次に、プレフィックス リストのシーケンス番号付けをディセーブルにする例を示します。

```
hostname(config)# no prefix-list sequence-number
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **prefix-list** | ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。 |
| **show running-config prefix-list** | 実行コンフィギュレーション内の **prefix-list** コマンドを表示します。 |

# pre-shared-key

事前共有キーを指定して、事前共有キーに基づく IKE 接続をサポートするには、トンネル グループ IPSec 属性コンフィギュレーション モードで **pre-shared-key** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**pre-shared-key** *key*

**no pre-shared-key**

## 構文の説明

| | |
|---|---|
| *key* | 1 ～ 128 文字の英数字キーを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| トンネル グループ ipsec 属性コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

この属性は、すべての IPSec トンネル グループ タイプに適用できます。

## 例

次に、設定 IPSec コンフィギュレーション モードで、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループの IKE 接続をサポートするように事前共有キー XYZX を指定する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear-configure tunnel-group** | 設定されているすべてのトンネル グループをクリアします。 |
| **show running-config tunnel-group** | すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。 |
| **tunnel-group ipsec-attributes** | このグループのトンネル グループ ipsec 属性を設定します。 |

# primary

プライマリ ユニットにフェールオーバー グループで高いプライオリティを指定するには、フェールオーバー グループ コンフィギュレーション モードで **primary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

**primary**

**no primary**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

フェールオーバー グループに **primary** または **secondary** が指定されていない場合は、フェールオーバー グループはデフォルトで **primary** に設定されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| フェールオーバー グループ コンフィギュレーション | • | • | — | — | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

プライマリまたはセカンダリのプライオリティをフェールオーバー グループに割り当てると、両方のユニットが（ユニットのポーリング期間内で）同時にブートしたときに、フェールオーバー グループがどのユニット上でアクティブになるかが指定されます。あるユニットがもう一方のユニットよりも先にブートした場合、両方のフェールオーバー グループがそのユニットでアクティブになります。もう一方のユニットがオンラインになったとき、2 番めのユニットをプライオリティの高いユニットとして所有するフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。

## 例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
```

```
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **failover group** | Active/Active フェールオーバーのためのフェールオーバー グループを定義します。 |
| **preempt** | 優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。 |
| **secondary** | セカンダリ ユニットにプライマリ ユニットよりも高いプライオリティを指定します。 |

# priority

QoS プライオリティ キューイングをイネーブルにするには、クラス コンフィギュレーション モードで **priority** コマンドを使用します。Voice over IP（VoIP）のように遅延を許容できないクリティカルなトラフィックでは、常に最低レートで送信されるように Low Latency Queueing（LLQ; 低遅延キューイング）のトラフィックを特定できます。プライオリティの要件を削除するには、このコマンドの **no** 形式を使用します。

**priority**

**no priority**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や変数はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| クラス | • | • | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

セキュリティ アプライアンスは、次の 2 タイプのプライオリティ キューイングをサポートしています。

- 標準プライオリティ キューイング：標準プライオリティ キューイングではインターフェイスで LLQ プライオリティ キューを使用しますが（**priority-queue** コマンドを参照）、他のすべてのトラフィックは「ベスト エフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになることを避けるには、キューのバッファ サイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。
- 階層型プライオリティ キューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キュー（**shape** コマンド）がイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。階層型プライオリティ キューイングについては、次のガイドラインを参照してください。

- プライオリティ パケットは常にシェープ キューの先頭に格納されるので、常に他の非プライオリティ キュー パケットよりも前に送信されます。
- プライオリティ トラフィックの平均レートがシェープ レートを超えない限り、プライオリティ パケットがシェープ キューからドロップされることはありません。
- IPSec-encrypted パケットの場合、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。
- プライオリティ トラフィック分類では、IPSec-over-TCP はサポートされません。

### Modular Policy Framework を使用した QoS の設定

プライオリティ キューイングをイネーブルにするには、Modular Policy Framework を使用します。標準プライオリティ キューイングまたは階層型プライオリティ キューイングを使用できます。

標準プライオリティ キューイングの場合は、次の作業を実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングをイネーブルにします。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

階層型プライオリティ キューイングの場合は、次の作業を実行します。

1. **class-map**：プライオリティ キューイングを実行するトラフィックを指定します。
2. **policy-map**（プライオリティ キューイングの場合）：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. **priority**：クラス マップのプライオリティ キューイングをイネーブルにします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。
3. **policy-map**（トラフィック シェーピングの場合）：**class-default** クラス マップに関連付けるアクションを指定します。
   a. **class class-default**：アクションを実行する **class-default** クラス マップを指定します。
   b. **shape**：トラフィック シェーピングをクラス マップに適用します。
   c. **service-policy**：プライオリティ キューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシー マップを呼び出します。
4. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

**例**

次に、ポリシー マップ モードでの **priority** コマンドの例を示します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)#
```

## 関連コマンド

| | |
|---|---|
| **class** | トラフィック分類に使用するクラス マップを指定します。 |
| **clear configure policy-map** | すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# priority（vpn ロード バランシング）

仮想ロード バランシング クラスタに参加するローカル デバイスのプライオリティを設定するには、VPN ロード バランシング モードで **priority** コマンドを使用します。デフォルトのプライオリティ指定に戻すには、このコマンドの **no** 形式を使用します。

**priority** *priority*

**no priority**

## 構文の説明

| | |
|---|---|
| *priority* | このデバイスに割り当てるプライオリティ（1 ～ 10 の範囲）。 |

## デフォルト

デフォルトのプライオリティは、デバイスのモデル番号によって異なります。

| モデル番号 | デフォルトのプライオリティ |
|---|---|
| 5520 | 5 |
| 5540 | 7 |

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| VPN ロード バランシング | — | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング モードを開始する必要があります。

このコマンドは、仮想ロード バランシング クラスタに参加するローカル デバイスのプライオリティを設定します。

プライオリティは、1（最低）～ 10（最高）の範囲の整数である必要があります。

プライオリティは、VPN ロード バランシング クラスタ内でクラスタのマスターまたはプライマリ デバイスになるデバイスを決定する方法の 1 つとして、マスター選出プロセスで使用されます。マスター選出プロセスの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

プライオリティ指定をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

## 例

次に、現在のデバイスのプライオリティを 9 に設定する **priority** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **vpn load-balancing** | VPN ロード バランシング モードを開始します。 |

# priority-queue

**priority** コマンドで使用するインターフェイスで標準プライオリティ キューを作成するには、グローバル コンフィギュレーション モードで **priority-queue** コマンドを使用します。キューを削除するには、このコマンドの **no** 形式を使用します。

**priority-queue** *interface-name*

**no priority queue** *interface-name*

## 構文の説明

| | |
|---|---|
| *interface-name* | プライオリティ キューをイネーブルにする物理インターフェイスの名前を指定します。ASA 5505 の場合は、VLAN インターフェイスの名前を指定します。 |

## デフォルト

デフォルトでは、プライオリティ キューイングはディセーブルです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0(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

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

セキュリティ アプライアンスは、次の 2 タイプのプライオリティ キューイングをサポートしています。

- 標準プライオリティ キューイング：標準プライオリティ キューイングでは、インターフェイスで **priority-queue** コマンドを使用して作成する LLQ プライオリティ キューを使用しますが、他のすべてのトラフィックは「ベスト エフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これは*テール ドロップ*と呼ばれます。キューがいっぱいになるのを回避するために、キューのバッファ サイズを増やすことができます（**queue-limit** コマンド）。また、送信キュー内に受け入れ可能な最大パケット数を微調整することもできます（**tx-ring-limit** コマンド）。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

- 階層型プライオリティ キューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キューがイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。

ASA モデル 5505（のみ）では、1 つのインターフェイスにプライオリティ キューを設定すると、他のすべてのインターフェイスで同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけが、すべてのインターフェイスに存在することになります。さらに、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスからも削除されます。

この問題を回避するには、**priority-queue** コマンドを 1 つのインターフェイスにのみ設定します。**queue-limit** コマンドと **tx-ring-limit** コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

## 例

次に、test という名前のインターフェイスに対してプライオリティ キューを設定し、キュー制限に 30,000 パケット、送信キュー制限に 256 パケットを指定する例を示します。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **queue-limit** | プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。 |
| **tx-ring-limit** | イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。 |
| **policy-map** | ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。 |
| **clear configure priority-queue** | 現在のプライオリティ キュー コンフィギュレーションを削除します。 |
| **show running-config [all] priority-queue** | 現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティ キュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。 |

# privilege

コマンド認可（ローカル、RADIUS、および LDAP（マッピング）のみ）で使用するコマンド特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。コンフィギュレーションを拒否するには、このコマンドの **no** 形式を使用します。

**privilege** [ **show** | **clear** | **configure** ] **level** *level* [ **mode** {**enable** | **configure**}] **command** *command*

**no privilege** [ **show** | **clear** | **configure** ] **level** *level* [ **mode** {**enable** | **configure**}] **command** *command*

## 構文の説明

| | |
|---|---|
| **clear** | （任意）コマンドの clear 形式に対してのみ特権を設定します。**clear**、**show**、**configure** キーワードのいずれも使用しない場合、このコマンドのすべての形式が影響を受けます。 |
| **command** *command* | 設定するコマンドを指定します。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。<br><br>また、サブコマンドの特権レベルは main コマンドと別に設定することもできません。たとえば、**context** コマンドは設定できますが、**allocate-interface** コマンドは **context** コマンドから設定を継承するため、設定できません。 |
| **configure** | （任意）コマンドの configure 形式に対してのみ特権を設定します。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。**clear**、**show**、**configure** キーワードのいずれも使用しない場合、このコマンドのすべての形式が影響を受けます。 |
| **level** *level* | 特権レベルを指定します。有効な値は、0 ～ 15 です。特権レベルの番号が小さいと、特権レベルが低くなります。 |
| **mode enable** | （任意）1 つのコマンドをコンフィギュレーション モードだけでなくユーザ EXEC モードおよび特権 EXEC モードで入力することができ、このコマンドが各モードで異なるアクションを実行する場合は、これらのモードに別々に特権レベルを設定できます。**mode enable** キーワードでは、ユーザ EXEC モードと特権 EXEC モードの両方を指定します。 |
| **mode configure** | （任意）1 つのコマンドをコンフィギュレーション モードだけでなくユーザ EXEC モードおよび特権 EXEC モードで入力することができ、このコマンドが各モードで異なるアクションを実行する場合は、これらのモードに別々に特権レベルを設定できます。**mode configure** キーワードは、**configure terminal** コマンドを使用してアクセスするコンフィギュレーション モードを指定します。 |
| **show** | （任意）コマンドの show 形式に対してのみ特権を設定します。**clear**、**show**、**configure** キーワードのいずれも使用しない場合、このコマンドのすべての形式が影響を受けます。 |

## デフォルト

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは、レベル 15 です。

- **show checksum**
- **show curpriv**

- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。このようにしないと、ユーザはコンフィギュレーション モードに入ることができません。

すべての特権レベルを表示するには、**show running-config all privilege all** コマンドを参照してください。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | Cisco VSA CVPN3000-Privilege-Level を使用する RADIUS ユーザのサポートが追加されました。**ldap map-attributes** コマンドを使用して LDAP 属性を CVPN3000-Privilege-Level にマッピングすると、LDAP ユーザがサポートされます。 |

## 使用上のガイドライン

**privilege** コマンドを使用すると、**aaa authorization command LOCAL** コマンドを設定するときに、セキュリティ アプライアンス コマンドの特権レベルを設定できます。このコマンドで **LOCAL** キーワードを使用する場合でも、このキーワードによってローカル、RADIUS、および LDAP（マッピング）認可がイネーブルになります。

## 例

たとえば、**filter** コマンドには次の形式があります。

- **filter**（**configure** オプションで表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。たとえば、それぞれの形式を別々に設定するには、次のように指定します。

```
hostname(config)# privilege show level 5 command filter
hostname(config)# privilege clear level 10 command filter
hostname(config)# privilege cmd level 10 command filter
```

また、すべてのフィルタ コマンドを同じレベルに設定できます。

```
hostname(config)# privilege level 5 command filter
```

**show privilege** コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザ EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
hostname(config)# privilege cmd level 0 mode enable command enable
hostname(config)# privilege cmd level 15 mode cmd command enable
hostname(config)# privilege show level 15 mode cmd command enable
```

次に、追加のコマンド **configure** コマンドの例を示します。このコマンドでは **mode** キーワードを使用します。

```
hostname(config)# privilege show level 5 mode cmd command configure
hostname(config)# privilege clear level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode cmd command configure
hostname(config)# privilege cmd level 15 mode enable command configure
```

**（注）** この最後の行は、**configure terminal** コマンドで使用します。

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure privilege** | コンフィギュレーションから privilege コマンド ステートメントを削除します。 |
| **show curpriv** | 現在の特権レベルを表示します。 |
| **show running-config privilege** | コマンドの特権レベルを表示します。 |

# prompt

CLI プロンプトをカスタマイズするには、グローバル コンフィギュレーション モードで **prompt** コマンドを使用します。デフォルトのプロンプトに戻すには、このコマンドの **no** 形式を使用します。

**prompt** {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]}

**no prompt** [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**]

## 構文の説明

| | |
|---|---|
| **context** | （マルチ モードのみ）現在のコンテキストを表示します。 |
| **domain** | ドメイン名を表示します。 |
| **hostname** | ホスト名を表示します。 |
| **priority** | フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。プライオリティは **failover lan unit** コマンドを使用して設定します。 |
| **state** | 装置のトラフィック通過状態を表示します。state キーワードに対して、次の値が表示されます。<br>• [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。<br>• stby：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。<br>• [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。<br>• [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 |

## デフォルト

デフォルトのプロンプトはホスト名です。マルチ コンテキスト モードでは、ホスト名の後に現在のコンテキスト名が続きます（*hostname*/*context*）。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| グローバル コンフィギュレーション | • | • | • | — | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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**

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。要素はスラッシュ（/）で区切ります。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

プロンプトに情報を追加できるため、複数のモジュールがある場合に、どのセキュリティ アプライアンスにログインしているかを一目で確認できます。この機能は、フェールオーバー時に、両方のセキュリティ アプライアンスに同じホスト名が設定されている場合に便利です。

**例**

次に、プロンプトで使用可能なすべての要素を表示する例を示します。

```
hostname(config)# prompt hostname context priority state
```

プロンプトが次のストリングに変化します。

```
hostname/admin/pri/act(config)#
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **clear configure prompt** | 設定したプロンプトをクリアします。 |
| **show running-config prompt** | 設定したプロンプトを表示します。 |

# protocol-enforcement

ドメイン名、ラベル長、形式チェック（圧縮およびループ ポインタのチェックを含む）をイネーブルにするには、パラメータ コンフィギュレーション モードで **protocol-enforcement** コマンドを使用します。プロトコルの強制をディセーブルにするには、このコマンドの **no** 形式を使用します。

**protocol-enforcement**

**no protocol-enforcement**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

プロトコルの強制は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定していれば、イネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no protocol-enforcement** を明示的に記述する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| パラメータ コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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

状況によっては、コマンドがディセーブルであっても、プロトコルの強制が実行されます。これは、DNS リソース レコードの分類、NAT、TSIG チェックなど、他の目的で DNS リソース レコードの解析が必要なときに発生します。

## 例

次に、DNS インスペクション ポリシー マップ内でプロトコルの強制をイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-enforcement
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップのクラス マップ名を指定します。 |
| **class-map type inspect** | アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。 |
| **policy-map** | レイヤ 3/4 のポリシー マップを作成します。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# protocol http

CRL を取得するための許可された配布ポイント プロトコルとして HTTP を指定するには、ca-crl コンフィギュレーション モードで **protocol http** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。CRL 取得方法として許可した HTTP を削除するには、このコマンドの **no** 形式を使用します。

**protocol http**

**no protocol http**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの設定は、HTTP を許可します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Ca-CRL コンフィギュレーション | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 使用上のガイドライン

このコマンドを使用する場合は、HTTP ルールをパブリック インターフェイス フィルタに適用してください。

## 例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして HTTP を許可する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crl configure** | ca-crl コンフィギュレーション モードを開始します。 |
| **crypto ca trustpoint** | トラストポイント コンフィギュレーション モードを開始します。 |
| **protocol ldap** | CRL の取得方法として LDAP を指定します。 |
| **protocol scep** | CRL の取得方法として SCEP を指定します。 |

# protocol ldap

CRL を取得するための配布ポイント プロトコルとして LDAP を指定するには、ca-crl コンフィギュレーション モードで **protocol ldap** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

**protocol ldap**

**no protocol ldap**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの設定は、LDAP を許可します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| CRL コンフィギュレーション | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして LDAP を許可する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crl configure** | ca-crl コンフィギュレーション モードを開始します。 |
| **crypto ca trustpoint** | トラストポイント コンフィギュレーション モードを開始します。 |
| **protocol http** | CRL の取得方法として HTTP を指定します。 |
| **protocol scep** | CRL の取得方法として SCEP を指定します。 |

# protocol scep

CRL を取得するための配布ポイント プロトコルとして SCEP を指定するには、crl コンフィギュレーション モードで **protocol scep** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

**protocol scep**

**no protocol scep**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの設定は、SCEP を許可します。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| CRL コンフィギュレーション | • | • | • | • | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | このコマンドが導入されました。 |

## 例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして SCEP を許可する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crl configure** | ca-crl コンフィギュレーション モードを開始します。 |
| **crypto ca trustpoint** | トラストポイント コンフィギュレーション モードを開始します。 |
| **protocol http** | CRL の取得方法として HTTP を指定します。 |
| **protocol ldap** | CRL の取得方法として LDAP を指定します。 |

# protocol-object

プロトコル オブジェクト グループにプロトコル オブジェクトを追加するには、プロトコル コンフィギュレーション モードで **protocol-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

**protocol-object** *protocol*

**no protocol-object** *protocol*

## 構文の説明

| | |
|---|---|
| protocol | プロトコルの名前または番号。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| プロトコル コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 既存 | このコマンドは既存です。 |

## 使用上のガイドライン

**protocol-object** コマンドは、**object-group** コマンドとともに使用して、プロトコル コンフィギュレーション モードでプロトコル オブジェクトを定義します。

IP プロトコルの名前や番号は、*protocol* 引数を使用して指定できます。udp プロトコル番号は 17、tcp プロトコル番号は 6、egp プロトコル番号は 47 です。

## 例

次に、プロトコル オブジェクトを定義する例を示します。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **clear configure object-group** | すべての **object group** コマンドをコンフィギュレーションから削除します。 |
| **group-object** | ネットワーク オブジェクト グループを追加します。 |
| **network-object** | ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。 |
| **object-group** | コンフィギュレーションを最適化するためのオブジェクト グループを定義します。 |
| **show running-config object-group** | 現在のオブジェクト グループを表示します。 |

# protocol-violation

HTTP および NetBIOS インスペクションでプロトコル違反が発生したときのアクションを定義するには、パラメータ コンフィギュレーション モードで **protocol-violation** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

**protocol-violation action** [**drop** [**log**] | **log**]

**no protocol-violation action** [**drop** [**log**] | **log**]

## 構文の説明

| | |
|---|---|
| **drop** | プロトコルに準拠しないパケットをドロップすることを指定します。 |
| **log** | プロトコル違反をログに記録することを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| パラメータ コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.2(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、HTTP または NetBIOS ポリシー マップで設定できます。HTTP または NetBIOS パーサーが HTTP または NetBIOS メッセージの最初の数バイトで有効なメッセージを検出できない場合、syslog が発行されます。たとえば、チャンク エンコーディングの形式が不正であるためにメッセージを解析できない場合に、このような状況が発生します。

## 例

次に、ポリシー マップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
hostname(config)# policy-map type inspect http http_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation action drop
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **class** | ポリシー マップのクラス マップ名を指定します。 |
| **class-map type inspect** | アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。 |

| コマンド | 説明 |
|---|---|
| **policy-map** | レイヤ 3/4 のポリシー マップを作成します。 |
| **show running-config policy-map** | 現在のポリシー マップ コンフィギュレーションをすべて表示します。 |

# proxy-bypass

コンテンツの最低限の書き換えを実行し、書き換えるコンテンツのタイプ（外部リンクや XML）を指定するようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モードで **proxy-bypass** コマンドを使用します。プロキシのバイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

**proxy-bypass interface** *interface name* {**port** *port number*| **path-mask** *path mask*} **target** *url* **[rewrite {link | xml | none}]**

**no proxy-bypass interface** *interface name* {**port** *port number*| **path-mask** *path mask*} **target** *url* **[rewrite {link | xml | none}]**

## 構文の説明

| | |
|---|---|
| **host** | トラフィックの転送先ホストを示します。ホストの IP アドレスまたはホスト名を使用します。 |
| **interface** | プロキシ バイパス用の ASA インターフェイスを示します。 |
| *interface name* | ASA インターフェイスを名前で指定します。 |
| **link** | 絶対外部リンクの書き換えを指定します。 |
| **none** | 書き換えを指定しません。 |
| **path-mask** | 一致パターンを指定します。 |
| *path-mask* | 照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。<br>*****：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。<br>?：任意の 1 文字に一致します。<br>[!seq]：シーケンスにない任意の文字に一致します。<br>[seq]：シーケンス内の任意の文字に一致します。<br>最大 128 バイトです。 |
| **port** | プロキシ バイパス用に予約されているポートを示します。 |
| *port number* | プロキシ バイパス用に予約されているポート（大きい番号）を指定します。ポートの範囲は 20000 ～ 21000 です。1 つのプロキシ バイパス ルールのみにポートを使用できます。 |
| **rewrite** | （任意）書き換え用の追加ルール（none、または XML やリンクの組み合わせ）を指定します。 |
| **target** | トラフィックの転送先リモート サーバを示します。 |
| *url* | URL を **http(s)://***fully_qualified_domain_name*[:*port*] という形式で入力します。最大 128 バイトです。別のポートを指定しない限り、HTTP のポートは 80、HTTPS のポートは 443 です。 |
| **xml** | 書き換える XML コンテンツを指定します。 |

## デフォルト

デフォルトの動作や値はありません。

**コマンド モード**

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| WebVPN コンフィギュレーション | • | — | • | — | — |

**コマンド履歴**

| リリース | 変更内容 |
|---|---|
| 7.1(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**

プロキシ バイパスは、コンテンツの書き換えを最小限に実行して、アプリケーションおよび Web リソースの動作を向上させるために使用します。proxy-bypass コマンドは、セキュリティ アプライアンスを通過する特定の Web アプリケーションの処理方法を決定します。

このコマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートがセキュリティ アプライアンスにアクセスできるようにするために、ファイアウォール コンフィギュレーションの変更が必要になることがあります。この制限を回避するには、パス マスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、URL が www.mycompany.com/hrbenefits の場合、*hrbenefits* がパスです。同様に、URL が www.mycompany.com/hrinsurance の場合、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

**例**

次に、webvpn インターフェイス上のプロキシ バイパス用にポート 20001 を使用するようにセキュリティ アプライアンスを設定する例を示します。HTTP とそのデフォルト ポート 80 を使用してトラフィックを mycompany.site.com に転送し、XML コンテンツを書き換えます。

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://mycompany.site.com rewrite xml
```

次に、外部インターフェイスでのプロキシ バイパス用にパス マスク mypath/* を使用するようにセキュリティ アプライアンスを設定する例を示します。HTTP とそのデフォルト ポート 443 を使用してトラフィックを mycompany.site.com に転送し、XML およびリンク コンテンツを書き換えます。

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://mycompany.site.com rewrite xml,link
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **apcf** | 特定アプリケーションに使用する非標準ルールを指定します。 |
| **rewrite** | トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。 |

# proxy-ldc-issuer

TLS プロキシ ローカル ダイナミック証明書を発行するには、クリプト CA トラストポイント コンフィギュレーション モードで **proxy-ldc-issuer** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

**proxy-ldc-issuer**

**no proxy-ldc-issuer**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

デフォルトの動作や値はありません。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| クリプト CA トラストポイント コンフィギュレーション | • | • | • | • | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが導入されました。 |

## 使用上のガイドライン

TLS プロキシ ローカル ダイナミック証明書を発行するには、**proxy-ldc-issuer** コマンドを使用します。**proxy-ldc-issuer** コマンドは、クリプト トラストポイントにローカル CA としてのロールを付与して LDC を発行します。クリプト ca トラストポイント コンフィギュレーション モードからアクセスできます。

**proxy-ldc-issuer** コマンドは、TLS プロキシのダイナミック証明書を発行するトラストポイントに、ローカル CA の役割を定義します。このコマンドは、「enrollment self」のトラストポイントにおいてのみ設定できます。

## 例

次に、内部ローカル CA を作成し、電話用の LDC を署名する例を示します。このローカル CA は、**proxy-ldc-issuer** がイネーブルな標準の自己署名トラストポイントとして作成されます。

```
hostname(config)# crypto ca trustpoint ldc_server
hostname(config-ca-trustpoint)# enrollment self
hostname(config-ca-trustpoint)# proxy-ldc-issuer
hostname(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
hostname(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
hostname(config-ca-trustpoint)# keypair ldc_signer_key
hostname(config)# crypto ca enroll ldc_server
```

**関連コマンド**

| コマンド | 説明 |
|---|---|
| **ctl-provider** | CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。 |
| **server trust-point** | TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。 |
| **show tls-proxy** | TLS プロキシを表示します。 |
| **tls-proxy** | TLS プロキシ インスタンスを定義し、最大セッション数を設定します。 |

# proxy-server

電話プロキシ機能に対して HTTP プロキシを設定するには、電話プロキシ コンフィギュレーション モードで **proxy-server** コマンドを使用します。このコンフィギュレーションは、IP フォンのコンフィギュレーション ファイルの <proxyServerURL> タグの下に書き込まれます。電話プロキシから HTTP プロキシ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

**proxy-server address** *ip_address* [*listen_port*] **interface** *ifc*

**no proxy-server address** *ip_address* [*listen_port*] **interface** *ifc*

## 構文の説明

| | |
|---|---|
| **interface** *ifc* | セキュリティ アプライアンスで HTTP プロキシが常駐するインターフェイスを指定します。 |
| *ip_address* | HTTP プロキシの IP アドレスを指定します。 |
| *listen_port* | HTTP プロキシのリスニング ポートを指定します。指定しない場合、デフォルトは 8080 になります。 |

## デフォルト

リッスン ポートを指定しない場合、ポートはデフォルトで 8080 に設定されます。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| Phone-Proxy コンフィギュレーション | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(4) | このコマンドが追加されました。 |

## 使用上のガイドライン

電話プロキシのプロキシ サーバ コンフィギュレーション オプションを設定すると、DMZ または外部ネットワークで HTTP プロキシを使用できます。これらのネットワークでは、電話機上のサービスについてすべての IP フォンの URL がこのプロキシ サーバに誘導されます。この設定では、非セキュアな HTTP トラフィックに対応します。このようなトラフィックは社内ネットワークに入ることはできません。

入力する *ip_address* は、IP フォンおよび HTTP プロキシ サーバの配置場所に基づくグローバル IP アドレスにする必要があります。

プロキシ サーバが DMZ 内にあり、IP 電話がネットワークの外部にある場合、セキュリティ アプライアンスは、NAT ルールが存在するかどうかのルックアップを実行し、グローバル IP アドレスを使用してコンフィギュレーション ファイルに書き込みます。

セキュリティ アプライアンスがホスト名を IP アドレスに解決できる場合は（DNS ルックアップが設定されている場合など）、セキュリティ アプライアンスがそのホスト名を IP アドレスに解決するため、*ip_address* 引数にホスト名を入力できます。

デフォルトでは、エンタープライズ パラメータの下に設定された電話の URL パラメータは、URL 内で FQDN を使用しています。HTTP プロキシ用の DNS lookup で FQDN が解決されない場合は、IP アドレスを使用するようにこれらのパラメータを変更する必要があります。

プロキシ サーバ URL が IP フォンのコンフィギュレーション ファイルに正しく書き込まれたかどうかを確認するには、[Settings] > [Device Configuration] > [HTTP configuration] > [Proxy Server URL] で IP フォンの URL をチェックします。

電話プロキシでは、プロキシ サーバに対するこの HTTP トラフィックを検査しません。

セキュリティ アプライアンスが IP フォンと HTTP プロキシ サーバのパス内にある場合は、既存のデバッグ手法（syslog やキャプチャなど）を使用して、プロキシ サーバをトラブルシューティングします。

電話プロキシが使用中の場合は、プロキシ サーバを 1 つだけ設定できます。ただし、プロキシ サーバを設定した後に IP 電話にコンフィギュレーション ファイルをダウンロードした場合は、IP 電話を再起動して、プロキシ サーバのアドレスが記載されたコンフィギュレーション ファイルが取り込まれるようにする必要があります。

## 例

次に、**proxy-server** コマンドを使用して電話プロキシ用に HTTP プロキシ サーバを設定する例を示します。

```
hostname(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **phone-proxy** | Phone Proxy インスタンスを設定します。 |

# publish-crl

ローカル CA が発行した証明書の失効状態を他のセキュリティ アプライアンスが検証できるようにするには、設定 CA サーバ コンフィギュレーション モードで **publish-crl** コマンドを使用します。このコマンドにより、セキュリティ アプライアンスのインターフェイスから CRL を直接ダウンロードできるようになります。CRL をダウンロードできないようにするには、このコマンドの **no** 形式を使用します。

**[ no ] publish-crl interface** *interface* **[ port** *portnumber* **]**

## 構文の説明

| | |
|---|---|
| **interface** *interface* | インターフェイスに使用される *nameif* を指定します（**gigabitethernet0/1** など）。詳細については、**interface** コマンドを参照してください。 |
| **port** *portnumber* | 任意。インターフェイス デバイスで CRL をダウンロードするときに使用するポートを指定します。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。 |

## デフォルト

デフォルトの **publish-crl** ステータスは、**no publish** です。TCP ポート 80 は、HTTP のデフォルトです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 設定 CA サーバ | • | — | • | — | — |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 8.0(2) | このコマンドが追加されました。 |

## 使用上のガイドライン

CRL は、デフォルトでアクセス不可です。必要なインターフェイスおよびポートで CRL ファイルへのアクセスをイネーブルにする必要があります。

TCP ポート 80 は、HTTP のデフォルト ポート番号です。デフォルト以外のポート（ポート 80 以外）を設定する場合は、他のデバイスが新しいポートへのアクセス方法を認識できるように、**cdp-url** コンフィギュレーションにそのポート番号が含まれるようにします。

CRL Distribution Point（CDP; CRL 配布ポイント）は、ローカル CA セキュリティ アプライアンスにおける CRL の場所です。cdp-url コマンドで設定する URL は、発行されるすべての証明書に埋め込まれます。CDP 用に特定の場所を設定しない場合、デフォルトの CDP の URL は http://hostname.domain/+CSCOCA+/asa_ca.crl です。

クライアントレス SSL VPN が同じインターフェイスでイネーブルになっている場合、HTTP リダイレクトと CRL ダウンロード要求は、同じ HTTP リスナーによって処理されます。リスナーは着信 URL をチェックし、cdp-url コマンドで設定した URL と一致する場合に、CRL ファイルがダウンロードされます。URL が cdp-url と一致しない場合は、接続が HTTPS にリダイレクトされます（「http redirect」がイネーブルの場合）。

## 例

次に、設定 CA サーバ モードで、外部インターフェイスのポート 70 を CRL ダウンロード用にイネーブルにする publish-crl コマンドの例を示します。

次に、設定 CA サーバ モードで、外部のポート 70 を CRL ダウンロード用にイネーブルにする **publish-crl** コマンドの例を示します。

```
hostname(config)# crypto ca server
hostname (config-ca-server)#publish-crl outside 70
hostname(config-ca-server)#
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **cdp-url** | 自動生成される CRL 用に特定の場所を指定します。 |
| **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。 |

# pwd

現在の作業ディレクトリを表示するには、特権 EXEC モードで **pwd** コマンドを使用します。

**pwd**

## 構文の説明

このコマンドには引数またはキーワードはありません。

## デフォルト

ルート ディレクトリ（/）がデフォルトです。

## コマンド モード

次の表に、コマンドを入力できるモードを示します。

| | ファイアウォール モード | | セキュリティ コンテキスト | | |
|---|---|---|---|---|---|
| | | | | マルチ | |
| コマンド モード | ルーテッド | 透過 | シングル | コンテキスト | システム |
| 特権 EXEC | • | • | • | — | • |

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 7.0 | 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、**dir** コマンドと機能が類似しています。

## 例

次に、現在の作業ディレクトリを表示する例を示します。

```
hostname# pwd
disk0:/
hostname# pwd
flash:
```

**関連コマンド**

| コマンド | 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** | ディレクトリの内容を表示します。 |
| **more** | ファイルの内容を表示します。 |