CHAPTER 22

packet-tracer コマンド～ pwd コマンド

packet-tracer

パケット トレース機能をイネーブルにして、パケットのスニッフィングやネットワーク障害切り離しを検出できるようにするには、**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

シンタックスの説明

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。利用できるプロトコル タイプのキーワードは、*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	（オプション）詳細なパケット トレース情報を提供します。
xml	（オプション）XML 形式でトレース キャプチャを表示します。

デフォルト

このコマンドにデフォルト設定はありません。

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
特権モード	•	—	•	•	•

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、パケットが予想どおりに動作しているかどうか確認するために、セキュリティ アプライアンスを通してパケットの寿命をトレースすることができます。**packet-tracer** コマンドを使用すると、次の処理を実行できます。

- 実稼働ネットワークのすべてのパケット ドロップをデバッグする。
- 設定が目的どおりに動作しているかどうかを確認する。
- ルールの追加の原因となった CLI 行に沿ってパケットに適用されるすべてのルールを表示する。
- データ パスにパケット変更のタイム ラインを表示する。
- トレーサー パケットをデータ パスに挿入する。

packet-tracer コマンドはパケットと、パケットがセキュリティ アプライアンスによりどのように処理されたかを示す詳細情報を提供します。このコンフィギュレーションからのコマンドによりパケットがドロップしないインスタンスでは、**packet-tracer** コマンドはその原因に関する情報を簡単に読み取れる方法で提供します。たとえば、無効なヘッダー確認が原因でパケットがドロップした場合、「不正な IP ヘッダーによりパケットがドロップしました（原因）」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 から詳細情報を持つ外部ホスト 209.165.202.158 に対するパケット トレースをイネーブルにするには、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	オプションが何も指定されていない場合は、キャプチャの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したときに表示される 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 モードで **page style** コマンドを使用します。

page style *value*

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

コマンドをコンフィギュレーションから削除し、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。

シンタックスの説明

value	Cascading Style Sheet（CSS）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
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現されます。このパラメータの説明は、このマニュアルでは取り扱いません。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 で入手可能です。

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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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 を使用することをお勧めします。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のに便利な機能があります。

例

次の例では、ページ スタイルを large にカスタマイズします。

```
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*

シンタックスの説明

[**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、ページが無制限であることを示します。範囲は 0 ～ 2,147,483,647 行です。**lines** キーワードはオプションです。このキーワードの有無にかかわらず、コマンドは同じです。

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
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 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 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 コマンドとして追加されました。

使用上のガイドライン

このコマンドにより、Telnet セッションでのデフォルトの pager line 設定を変更します。現行セッションに対してのみ一時的に設定を変更する場合は、**terminal pager** コマンドを使用します。

管理コンテキストに Telnet 接続する場合、ある特定のコンテキスト内の **pager** コマンドに異なる設定があっても、他のコンテキストに移ったときには、pager line 設定はユーザの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

次の例では、表示される行数を 20 に変更します。

```
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消去します。
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージが Telnet セッションで表示されるようにします。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードで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 モードに入り、検査ポリシー 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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 フレームワークを利用すると、数多くのアプリケーション検査のための特別なアクションを設定できます。**inspect** コマンドを使用して、レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で検査エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成した検査ポリシー マップで定義するアクションを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、検査ポリシー マップの名前です。

検査ポリシー マップは 1 つまたは複数の **parameters** コマンドをサポートできます。パラメータは検査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

次の例では、デフォルトの検査ポリシー マップ内に DNS パケットの最大メッセージ長を設定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)# message-length maximum 512
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

participate

デバイスを仮想ロードバランシング クラスタに強制的に参加させるには、VPN ロードバランシング モードで **participate** コマンドを使用します。クラスタに参加した状態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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト動作では、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
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

VPN ロードバランシング モードに入るには、**interface** コマンドおよび **nameif** コマンドを使用してインターフェイスを設定してから、**vpn load-balancing** コマンドを使用する必要があります。また、事前に **cluster ip** コマンドを使用してクラスタの IP アドレスを設定し、仮想クラスタの IP アドレスが参照するインターフェイスを設定する必要があります。

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。

1 つのクラスタに参加しているすべてのデバイスの IP アドレス、暗号化設定、暗号キー、およびポートの値は、クラスタ固有の同一の値である必要があります。

（注） 暗号化を使用する場合は、事前に **isakmp enable** *inside* コマンドを設定する必要があります。*inside* には、ロードバランシング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内部インターフェイス上で isakmp がイネーブルになっていないと、クラスタ暗号化の設定を試みたときにエラー メッセージが表示されます。

cluster encryption コマンドを設定したときには isakmp がイネーブルであっても、**participate** コマンドを設定する前にディセーブルになった場合は、**participate** コマンドの入力時にエラー メッセージが表示され、そのローカル デバイスはクラスタに参加しません。

例

次に、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。これには、現在のデバイスが 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** コマンドが含まれています。

```
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
hostname(config-load-balancing)#
```

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 モードに入ります。

passive-interface

インターフェイスでの RIP ルーティング アップデートの伝送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の RIP ルーティング アップデートをもう一度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*}

シンタックスの説明

default	(オプション)すべてのインターフェイスをパッシブ モードに設定します。
if_name	(オプション)RIP がパッシブ モードに設定されるインターフェイスです。

デフォルト

すべてのインターフェイスは RIP がイネーブルの場合にアクティブ RIP に対してイネーブルになります。

インターフェイスまたは **default** キーワードが指定されていない場合、コマンドは ***default*** がデフォルト設定となり、`passive-interface default` としてコンフィギュレーションに表示されます。

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
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

パッシブ RIP をインターフェイスで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 テーブルに値を挿入しますが、ルーティング アップデートをブロードキャストしません。

例

次の例では、外部インターフェイスをパッシブ RIP に設定します。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 アップデートを送受信します。

```
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 コマンドを消去します。
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 モードに入ります。
show running-config rip	実行コンフィギュレーション内の RIP 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、CLI にデフォルト ユーザとしてアクセスするときは、ログイン パスワードを入力するためのプロンプトが表示されます。ログイン パスワードを入力すると、ユーザ EXEC モードに入ります。

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

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

シンタックスの説明

encrypted	（オプション）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のに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使用して **passwd** コマンドを入力します。通常、このキーワードは、**show running-config passwd** コマンドを入力した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	パスワードに、大文字と小文字が区別される最大 80 文字の文字列を設定します。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 パスワードは「cisco」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
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のものです。

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 ユーザ用です。**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 認証を設定した場合、このパスワードは使用されません。

例

次の例では、パスワードを Pa$$w0rd に設定します。

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

次の例では、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をパスワードに設定します。

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

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
enable	特権 EXEC モードに入ります。
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の名前および特権レベルを表示します。
show running-config passwd	ログイン パスワードを暗号化された形で表示します。

password（暗号 CA トラストポイント）

登録中に CA に登録するチャレンジ フレーズを指定するには、暗号 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。CA は、通常、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

シンタックスの説明

string	パスワードの名前を文字列として指定します。最初の文字を数字にすることはできません。文字列には、スペースを含む最大 80 文字の任意の英数字を使用できます。数字、スペース、任意の文字という形式のパスワードは指定できません。数字の後にスペースがあると、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」は不適切です。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、「Secret」というパスワードと「secret」というパスワードは異なります。

デフォルト

デフォルトでは、パスワードを含めない設定になっています。

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
暗号 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(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

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書の失効パスワードを指定できます。指定したパスワードは、アップデート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になっていない場合、証明書登録中にパスワードの入力は求められません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、CA に登録するチャレンジ フレーズをトラストポイント central の登録要求に含めています。

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

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 モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

password-management

パスワード管理をイネーブルにするには、トンネル グループ一般アトリビュート 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、***password-expire-in-days*** キーワードを指定してこのコマンドの **no** 形式を使用します。

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

no password-management

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

シンタックスの説明

days	現行のパスワードが期限切れになるまでの日数（0 ～ 180）を指定します。このパラメータは、***password-expire-in-days*** キーワードを指定する場合には必須です。
password-expire-in-days	（オプション）この直後のパラメータにより、現行のパスワードが期限切れになるまでの日数が指定され、セキュリティ アプライアンスが、ユーザにパスワードの期限が切れる時期が迫っていることを知らせる警告を開始します。このオプションは、LDAP サーバに対してのみ有効です。

デフォルト

このコマンドを指定しない場合、パスワード管理は行われません。***password-expire-in-days*** キーワードを指定しない場合、警告が開始されてから現行のパスワードが期限切れとなるまでのデフォルトの期間は 14 日間です。

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
トンネル グループ一般アトリビュート 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

このアトリビュートは、IPSec リモート アクセスおよび WebVPN トンネル グループに設定できます。

このコマンドを設定すると、ログイン時にセキュリティ アプライアンスはリモート ユーザに、ユーザの現行のパスワードの期限が切れようとしている、またはパスワードが失効したということを通知します。ここでユーザは、セキュリティ アプライアンスにより、パスワードを変更する機会が与えられます。現行のパスワードがまだ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できます。このコマンドは、このような通知をサポートする AAA サーバ（つまり、RADIUS サーバ、NT サーバを使用する RADIUS サーバ、および LDAP サーバ）に有効です。RADIUS または LDAP 認証が設定されていない場合、このコマンドはセキュリティ アプライアンスで無視されます。

このコマンドは、パスワードの期限が切れ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パスワードの期限が切れようとしているという警告を発した日から期限切れの日までの日数を変更するものであること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、この日数も指定する必要があります。

この日数を 0 に設定してこのコマンドを指定すると、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、期限が迫っていることをユーザに通知しませんが、期限が切れた後で、ユーザはパスワードを変更できます。

例

次の例では、WebVPN トンネル グループ「testgroup」のパスワードの期限が切れる 90 日前になるとユーザに警告を開始するように設定します。

```
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)#
```

次の例では、デフォルト値を使用して IPSec リモート アクセス トンネル グループ「QAgroup」のユーザにパスワードの期限が切れる 14 日前から警告を開始するようにします。

```
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 パスワードを消去します。
passwd	ログイン パスワードを設定します。
radius-with-expiry	RADIUS 認証の間にパスワード アップデートのネゴシエーションをイネーブルにします（これは廃止されました）。
show running-config passwd	ログイン パスワードを暗号化された形で表示します。
tunnel-group general-attributes	トンネル グループ一般アトリビュート値を設定します。

password-parameter

SSO 認証用にユーザ パスワード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 Forms コマンドを使用した SSO です。

password-parameter *string*

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	HTTP POST 要求に含まれるパスワード パラメータの名前です。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
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、認証 Web サーバに対してシングル サインオン認証要求を送信するために HTTP POST 要求を使用します。必要とされるコマンド **password-parameter** は、この POST 要求が 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。このパスワードは POST 要求に入力されて認証 Web サーバに渡されます。

例

次の例では、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 パラメータを指定します。

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

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とパスワードを受信する 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 サーバとの交換に使用する非表示パラメータを作成します。
start-url	事前ログイン クッキーの取得先 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 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 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*

コマンドをコンフィギュレーションから削除し、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。

シンタックスの説明

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のテキストは「PASSWORD:」です。

パスワード プロンプトのデフォルトのスタイルは、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
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現されます。このパラメータの説明は、このマニュアルでは取り扱いません。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 で入手可能です。

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）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目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 を使用することをお勧めします。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のに便利な機能があります。

例

次の例では、テキストを「Corporate Password:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更しています。

```
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

クライアント システム上にログイン パスワードを保存することをユーザに許可するには、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。パスワードの保存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。

password-storage アトリビュートを実行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** 形式を使用します。これにより、password-storage の値を別のグループ ポリシーから継承できるようになります。

password-storage {enable | disable}

no password-storage

シンタックスの説明

disable	パスワードの保存をディセーブルにします。
enable	パスワードの保存をイネーブルにします。

デフォルト

パスワードの保存はディセーブルになっています。

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
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(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

セキュアなサイトにあることが判明しているシステムに限り、パスワードの保存をイネーブルにしてください。

このコマンドは、対話型ハードウェア クライアント認証またはハードウェア クライアントの個別ユーザ認証とは関係ありません。

例

次の例は、FirstGroup というグループ ポリシーのパスワードの保存をイネーブルにする方法を示しています。

```
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アイデンティティを確認するかどうかを指定するには、トンネル グループ ipsec アトリビュート 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

シンタックスの説明

option	次のオプションのいずれかを指定します。 • ***req***：必須 • ***cert***：証明書によってサポートされている場合 • ***nocheck***：確認しない

デフォルト

デフォルトでは、このコマンドの設定は ***req*** 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
トンネル グループ IPSec アトリビュート	•	—	•	—	—

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

このアトリビュートは、すべての IPSec トンネル グループ タイプに適用できます。

例

config-ipsec コンフィギュレーション モードで入力された次の例は、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループのピアの証明書のアイデンティティを使用してのピアの確認を要求します。

```
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 グループを消去します。
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 アトリビュートを設定します。

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***]

シンタックスの説明

verbose	セキュリティ アプライアンス コンソールにパフォーマンス モニタ情報を表示します。
interval *seconds*	コンソールの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 モニタの表示をディセーブルにします。
settings	interval を表示し、quiet と verbose のいずれ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
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	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*** キーワードがサポートされるようになりました。

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監視できます。情報をすぐに表示するには、**show perfmon** コマンドを使用します。情報を 2 分間隔で表示し続けるには、**perfmon verbose** コマンドを使用します。指定した秒間隔で情報を表示し続けるには、**perfmon interval** *seconds* コマンドと **perfmon verbose** コマンドを併用します。

パフォーマンス情報は次のように表示されます。

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

この情報では、変換、接続、Websense 要求、アドレス変換（「フィックスアップ」と呼ばれる）、および AAA トランザクションについて、毎秒発生する数が表示されます。

例

次の例は、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方法を示しています。

```
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*

シンタックスの説明

days-of-the-week	（オプション）最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（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。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 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、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

periodic コマンドに値が入力されていない場合、***time-range*** コマンドによる定義に従ったセキュリティ アプライアンスへのアクセスがすぐに有効になり、常時オンとなります。

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
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。その後、**access-list extended time-range** コマンドを使用して、時間範囲を ACL にバインドします。

periodic コマンドは、時間範囲をいつ有効にするかを指定する方法の 1 つです。別の方法は、***absolute*** コマンドを使用して絶対時間範囲を指定する方法です。これらのコマンドのいずれかを、***time-range*** グローバル コンフィギュレーション コマンドの後に使用します。このコマンドは、時間範囲の名前を指定します。***time-range*** コマンドあたり複数の ***periodic*** 値を入力できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、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*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 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。しかし、この機能は、NTP 同期化により最適に動作します。

例

次にいくつかの例を示します。

必要な設定	入力内容
月曜日から金曜日の午前 8 時～午後 6 時のみ	***periodic weekdays 8:00:00 to 18:00***
毎日午前 8 時～午後 6 時のみ	***periodic daily 8:00 to 18:00***
月曜日午前 8 時～金曜日午後 8 時の 1 分おき	***periodic monday 8:00 to friday 20:00***
週末、つまり土曜日の朝から日曜日の終わりまで	***periodic weekend 00:00:00 to 23:59***
土曜日および日曜日の正午～深夜	***periodic weekend 12:00:00 to 23:59***

次の例は、月曜日から金曜日の午前 8 時～午後 6 時にセキュリティ アプライアンスにアクセスすることを許可する方法を示しています。

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

次の例は、特定の曜日（月曜日、火曜日、および金曜日）の午前 10 時 30 分～午後 12 時 30 分にセキュリティ アプライアンスにアクセスすることを許可する方法を示しています。

```
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	時間範囲が有効である絶対時間を定義します。
access-list extended	セキュリティ アプライアンスを通して IP トラフィックの許可または拒否に対するポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元します。
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、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できます。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。

permit errors

no permit errors

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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

無効なパケット、またはセキュリティ アプライアンスを通じて送信されるメッセージの検査中にエラーが発生したパケットを許可し、それらがドロップされないようにするには、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。

例

次の例では、無効なパケットまたは解析中に失敗したパケットが含まれたトラフィックを許可します。

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

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
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	アプリケーション検査に使用する特定の 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できます。permit response コマンドは、応答の送信先であった GSN とは異なる GSN からの GTP 応答を許可することにより、ロードバランシング GSN をサポートします。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。

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*

シンタックスの説明

from-object-group *from_obj_group_id*	**object-group** コマンドにより設定された、*to_obj_group_id* 引数で指定したオブジェクト グループ内の GSN の集合に対して応答を送信できるオブジェクト グループの名前を指定します。セキュリティ アプライアンスがサポートしているのは、IPv4 アドレスを持つネットワーク オブジェクトを含んだオブジェクト グループのみです。IPv6 アドレスは、現時点では GTP でサポートされていません。
to-object-group *to_obj_group_id*	**object-group** コマンドにより設定された、*from_obj_group_id* 引数で指定したオブジェクト グループ内の GSN の集合から応答を受信できるオブジェクト グループの名前を指定します。セキュリティ アプライアンスがサポートしているのは、IPv4 アドレスを持つネットワーク オブジェクトを含んだオブジェクト グループのみです。IPv6 アドレスは、現時点では GTP で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、要求送信先のホスト以外の GSN からの GTP 応答をドロップします。

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
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)(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** コマンドを使用して、応答の送信先であった GSN とは異なる GSN からの、GTP 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 のプールをネットワーク オブジェクトとして指定します。同様に、SGSN をネットワーク オブジェクトとして指定します。応答する GSN が、GTP 要求の送信先であった GSN と同じオブジェクト グループに属する場合、また応答する GSN が GTP 応答を送信できるオブジェクト 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

次の例では、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 を持つホストへの GTP 応答を許可します。

```
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 GTP 統計情報を消去します。
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	アプリケーション検査に使用する特定の 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。PFS アトリビュートを実行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** 形式を使用します。このオプションを使用すると、PFS の値を別のグループ ポリシーから継承できます。

IPSec ネゴシエーションで、PFS は新しい暗号鍵が以前のどの鍵とも無関係であることを保証します。

pfs {enable | disable}

no pfs

シンタックスの説明

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 はディセーブルになっています。

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
グループ ポリシー	•	—	•	—	—

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

PFS 設定は、VPN クライアントとセキュリティ アプライアンスで一致している必要があります。

例

次の例は、FirstGroup というグループ ポリシーの PFS を設定する方法を示しています。

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

pim

インターフェイス上の PIM を再度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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

multicast-routing コマンドは、デフォルトで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
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

multicast-routing コマンドは、デフォルトで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。**no** 形式の **pim** コマンドだけ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

次の例では、選択したインターフェイス上の PIM をディセーブルにします。

```
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 アプライアンス上のマルチキャスト 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** 形式を使用します。

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

no pim accept-register

シンタックスの説明

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、標準ホスト ACL だけを使用してください。拡張 ACL はサポートされていません。
route-map *map-name*	ルートマップ名を指定します。参照先のルートマップでは、標準ホスト ACL を使用してください。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
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

非認証の送信元が RP に登録されないようにするには、このコマンドを使用します。非認証の送信元が 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中止メッセージを送信します。

例

次の例では、PIM 登録メッセージを、「no-ssm-range」というアクセス リストに定義されている送信元からのものに制限します。

```
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 アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim bidir-neighbor-filter

どの双方向対応ネイバーが DF 選定に参加できるかを制御するには、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** 形式を使用します。

pim bidir-neighbor-filter *acl*

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

シンタックスの説明

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 リストでは、双方向 DF 選定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 だけを使用してください。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判断されます。

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
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 を使用すると、マルチキャスト ルータでは、情報を縮小して保持できます。セグメント内のすべてのマルチキャスト ルータは、bidir で DF を選定できるよう双方向にイネーブルになっていなければなりません。

pim bidir-neighbor-filter コマンドを使用すると、希薄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、すべてのルータの希薄モード ドメインへの参加を許可しながら、DF 選定へ参加しなければならないルータを指定します。双方向対応のルータは、セグメントに双方向非対応のルータがある場合でも、ルータの中から DF を選定できます。双方向非対応のルータのマルチキャスト境界は、双方向対応のグループからの PIM メッセージとデータが、双方向対応のサブセット クラウド内外に漏れることを防ぎます。

pim bidir-neighbor-filter コマンドがイネーブルになっていると、ACL により許可されているルータは双方向対応であると考えられます。したがって、次のような結果になります。

- 許可されたネイバーが双方向に対応しない場合、DF 選定は発生しません。
- 拒否されたネイバーが双方向に対応する場合、DF 選定は発生しません。
- 拒否されたネイバーが双方向に対応しない場合、DF 選定が発生します。

例

次の例では、10.1.1.1 が PIM 双方向対応ネイバーになります。

```
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	管理用のマルチキャスト アドレスのマルチキャスト境界を定義します。
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim dr-priority

指定ルータの選定に使用されるネイバーの優先順位をセキュリティ アプライアンス上に設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトの優先順位に戻すには、このコマンドの **no** 形式を使用します。

pim dr-priority *number*

no pim dr-priority

シンタックスの説明

number	0 ～ 4294967294 の任意の数字。この数字は、指定ルータを判別するときに、デバイスの優先順位を判別するために使用されます。0 に指定すると、セキュリティ アプライアンスは指定ルータに選定されません。

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
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

インターフェイス上の優先順位値が最も大きいデバイスが、PIM 指定ルータになります。複数のデバイスで同じ指定ルータ優先順位値が設定されている場合、IP アドレスが最大のデバイスが指定ルータになります。デバイスの hello メッセージに DR-Priority Option（指定ルータ優先順位オプション）が含まれていない場合は、そのデバイスが最も優先順位の高いデバイスであると見なされ、指定ルータになります。hello メッセージにこのオプションが含まれていないデバイスが複数ある場合は、最大の IP アドレスを持つデバイスが指定ルータになります。

例

次の例は、インターフェイスの指定ルータ優先順位を 5 に設定します。

```
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 アプライアンス上のマルチキャスト 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 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 hello-interval *seconds*

no pim hello-interval [*seconds*]

シンタックスの説明

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前に待機する秒数。有効となる値の範囲は、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
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

次の例では、PIM hello 間隔を 1 分に設定します。

```
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 アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim join-prune-interval

PIM join/prune 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。この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*]

シンタックスの説明

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前に待機する秒数。有効となる値の範囲は、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
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

次の例では、PIM join/prune 間隔を 2 分に設定します。

```
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 アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim neighbor-filter

どのネイバ ルータが PIM 選定に参加できるかを制御するには、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** 形式を使用します。

pim neighbor-filter *acl*

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

シンタックスの説明

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 だけを使用してください。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
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、どのネイバー ルータが PIM に参加できるかを定義します。このコマンドがコンフィギュレーションに含まれていない場合、制限はありません。

このコマンドをコンフィギュレーション内に表示するには、マルチキャスト ルーティングと PIM がイネーブルでなければなりません。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

次の例では、IP アドレス 10.1.1.1 のルータが、GigabitEthernet0/2 インターフェイスで PIM ネイバーになるのを禁止します。

```
hostname(config)# access-list pim_filter deny 10.1.1.1 255.255.255.255
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 アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim old-register-checksum

古い登録チェックサム方法論を使用する Rendezvous Point（RP; ランデブー ポイント）上の下位互換性を許可するには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠の登録を生成するには、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

セキュリティ アプライアンスは、PIM RFC 準拠の登録を生成します。

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
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 ヘッダー上のチェックサムを持つ登録メッセージと、それに続く 4 バイトだけを受け入れます。つまり、登録メッセージをすべての PIM メッセージ タイプ用の PIM メッセージ全体と共に受け入れます。**pim old-register-checksum** コマンドは、Cisco IOS ソフトウェアと互換性のある登録を生成します。

例

次の例では、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 アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim rp-address

PIM Rendezvous Point（RP; ランデブー ポイント）のアドレスを設定するには、グローバル コンフィギュレーション モードで **pim 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*

シンタックスの説明

acl	（オプション）RP と共に使用するマルチキャスト グループを定義する、標準的なアクセス リストの名前または番号。このコマンドでホスト ACL を使用しないでください。
bidir	（オプション）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示します。このオプションを使用しないでコマンドを設定した場合、指定したグループは PIM 希薄モードで動作します。
ip_address	PIM RP として使用するルータの IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

このコマンドには、引数もキーワードもありません。

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
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

共通の PIM 希薄モード（PIM-SM）または双方向ドメイン内にあるすべてのルータは、周知の PIM RP アドレスの情報を必要とします。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します。

（注）　セキュリティ アプライアンスは、Auto-RP をサポートしていません。したがって、**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。

1 つの RP で複数のグループが処理されるように設定できます。アクセス リストで指定されているグループ範囲により、PIM RP グループ マッピングが決まります。アクセス リストが指定されていない場合、グループの RP は、IP マルチキャスト グループ範囲全体（224.0.0.0/4）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にかかわらず、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

次の例では、すべてのマルチキャスト グループの PIM RP アドレスに 10.0.0.1 を設定します。

```
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 登録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

最後のホップ ルータの動作を、常に共有ツリーを使用し、Shortest-Path Tree（SPT; 最短パス ツリー）への切り替えを決して実行しないように変更するには、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

シンタックスの説明

***group-list** acl*	（オプション）アクセス リストで制限されている送信元グループを指定します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされていません。

デフォルト

デフォルトでは、最後のホップ PIM ルータは最短パス送信元ツリーに切り替えます。

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
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

次の例では、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最後のホップ PIM ルータを設定します。

```
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 アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

ping

セキュリティ アプライアンスから他の IP アドレスが可視であ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**]

シンタックスの説明

***data** pattern*	（オプション）16 ビット データ パターンを 16 進数で指定します。
host	ping 対象のホストの IPv4 または IPv6 アドレス、または名前を指定します。この名前は DNS 名、または **name** コマンドで割り当てられた名前になります。DNA 名の最大文字数は 128 文字、**name** コマンドで作成した名前の最大文字数は 63 文字です。
if_name	（オプション）***nameif*** コマンドで設定され、*host* へのアクセスに使用できるインターフェイス名を指定します。指定しない場合、*host* は解決されて IP アドレスに変換され、その後で、宛先インターフェイスを確認するために、ルーティング テーブルが参照されます。
***repeat** count*	（オプション）ping 要求を繰り返す回数を指定します。
***size** bytes*	（オプション）データグラム サイズをバイト単位で指定します。
timeout *seconds*	（オプション）ping 要求がタイムアウトになるまでの秒数を指定します。
validate	（オプション）応答データを検証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
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のものです。
7.2(1)	DNS 名がサポートされるようになりました。

使用上のガイドライン

ping コマンドでは、セキュリティ アプライアンスに接続できるかどうか、またはホストがネットワークで利用可能であるかどうかが判断できます。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の応答および受け入れをセキュリティ アプライアンスに許可するために必要です。***ping*** コマンドの出力には、応答が受信されたかどうかが示されます。**ping** コマンドを入力したとき、ホストが応答していない場合は、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されていること、およびトラフィックの受け渡しを実行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* のアドレスは 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 ping を送信する場合は、次のいずれかを実行する必要があります。

- エコー応答用の ICMP ***access-list*** コマンドを作成します。たとえば、ping アクセスをすべてのホストに許可するには、***access-list acl_grp permit icmp any any*** コマンドを使用します。***access-group*** コマンドを使用して、テストの対象であるインターフェイスに ***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 検査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たエコー要求に対して、セキュリティ アプライアンスを経由したエコー応答が許可されます。

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

ホスト間またはルータ間でセキュリティ アプライアンスを介して ping を実行するが、ping が成功しない場合は、**capture** コマンドを使用して ping の成功を監視できます。

セキュリティ アプライアンス **ping** コマンドでは、インターフェイス名は必須ではありません。インターフェイス名が指定されていない場合、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て指定されたアドレスを検索します。インターフェイス名を指定して、ICMP エコー要求が送信されるときに経由するインターフェイスを指示できます。

例

次の例は、他の IP アドレスがセキュリティ アプライアンスから可視であるかどうかを判断する方法を示しています。

```
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
```

次の例は、DNS 名を使用するホストを指定します。

```
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 ping の例を示します。

```
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	インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
show interface	VLAN コンフィギュレーションについての情報を表示します。

police

厳密なスケジューリング優先順位をこのクラスに適用するには、クラス モードで **police** コマンドを使用します。レート制限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。

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

no police

シンタックスの説明

burst-size	1,000 ～ 512,000,000 の範囲の値。適合レート値にスロットリングするまでに持続的なバーストで許容される最大瞬間バイト数を指定します。
conform-action	レートが *burst-size* の値より小さいときに実行されるアクション（パケットのドロップまたは伝送）。
conform-rate	このトラフィック フローのレート限度。8,000 ～ 2,000,000,000 の任意の値で、許容される最大速度（ビット / 秒）を指定します。
drop	パケットをドロップします。
exceed-action	このアクションは、レートが conform-rate 値と conform-burst 値の間であるときに実行されます。
input	入力方向に流れるトラフィックのポリシングをイネーブルにします。
output	出力方向に流れるトラフィックのポリシングをイネーブルにします。
transmit	パケットを伝送します。

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。
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。コマンドの指定において、*conform rate* に続くコマンド内のすべてがオプションであることを示すシンタックスの表記方法が変更されました。

使用上のガイドライン

police コマンドを発行する前に、**policy-map** コマンドと **class** コマンドを設定しておく必要があります。

（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合せるだけです。***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。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（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。適合レート 100,000 ビット / 秒、バースト値 2,000,000 バイトを設定し、バースト レートを超過したトラフィックをドロップすることを指定しています。

```
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)#
```

次の例では、内部 Web サーバ宛のトラフィックに対してレート制限を設定する方法を示します。

```
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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

policy

CRL を取得するための送信元を指定するには、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*}

シンタックスの説明

both	CRL 配布ポイントを使用して CRL を取得することに失敗した場合は最大 5 つのスタティック CRL 配布ポイントを使用してリトライすることを、指定します。
cdp	チェック中の証明書に組み込まれた、CRL 配布ポイント拡張を使用します。この場合、セキュリティ アプライアンスは、チェック中の証明書の CRL 配布ポイント拡張から最大 5 つの CRL 配布ポイントを取得し、必要に応じて、設定されたデフォルト値で情報を増強します。セキュリティ アプライアンスは、プライマリ CRL 配布ポイントを使用して CRL を取得することに失敗した場合、リストにある次に利用可能な CRL 配布ポイントを使用してリトライします。これは、セキュリティ アプライアンスが CRL を取得するか、リストを使い果たすまで続行されます。
static	最大 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** コマンドで LDAP または HTTP URL も指定してください。

デフォルト

デフォルト設定は **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(1)	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、チェック中の証明書内の CRL 配布ポイントを使用して CRL 取得を実行すること、それに失敗した場合は、スタティック CRL 配布ポイントを使用することを設定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
url	CRL を取得するためのスタティック 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、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** キーワードなし）を使用し、レイヤ 3/4 クラス マップ（**class-map** コマンドまたは **class-map type management** コマンド）で特定したトラフィックにアクションを割り当てます。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*

シンタックスの説明

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 マップが同じネーム スペースを使用しているため、他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
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. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのため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、インターフェイスに対するアクションを有効にします。

ポリシー マップの最大数は 64 です。レイヤ 3/4 ポリシー マップ内の複数のレイヤ 3/4 クラス マップを指定でき（**class** コマンドを参照）、各クラス マップに 1 つまたは複数の機能タイプから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 マップ内にある 1 つのクラス マップだけに一致します。パケットがある機能タイプのクラス マップと一致すると、セキュリティ アプライアンスはそのクラス マップを、その機能タイプの後続のクラス マップと照合しません。パケットが別の機能タイプの後続のクラス マップと一致すると、セキュリティ アプライアンスはそのクラス マップのアクションも適用します。たとえば、パケットが接続制限のクラス マップと一致し、アプリケーション検査のクラス マップにも一致する場合、両方のクラス マップの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検査のクラス マップと一致するが、アプリケーション検査の別のクラス マップとも一致する場合、2 番目のクラス マップの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のトラフィックに適用されます。双方向に適用される機能については、トラフィックが双方向のクラス マップに一致する場合、ポリシー マップの適用先であるインターフェイスに入る、または出るすべてのトラフィックに影響します。

（注）　グローバル ポリシーを使用する場合、すべての機能は単方向です。1 つのインターフェイスに適用されるときに通常は双方向である機能は、グローバルに適用される際には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、ポリシーは双方向に適用されます。この場合の双方向性は冗長になります。

QoS など単方向に適用される機能の場合、ポリシーが適用されるインターフェイスを出るトラフィックのみ影響を受けます。各機能の方向性については、表 22-1 を参照してください。

表 22-1　機能の方向性

機能	一方向のインターフェイス	グローバルな方向
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
アプリケーション検査	双方向	入力
IPS	双方向	入力
QoS ポリシング	出力	出力
QoS プライオリティ キュー	出力	出力

ポリシー マップ内の各種アクションが実行される順序は、そのポリシー マップ内にアクションが出現する順序とは関係ありません。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 または CSC など）を実行する場合、または TCP ペイロード（FTP 検査など）を修正する場合、TCP ノーマライザはデュアル モードで動作します。このモードでは、ノーマライザはプロキシまたはペイロードの修正サービスの前後に適用されます。

- CSC
- アプリケーション検査
- IPS
- QoS ポリシング
- QoS プライオリティ キュー

各インターフェイスに割り当てられるポリシー マップは 1 つだけですが、複数のインターフェイスに同じポリシー マップを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、セキュリティ アプライアンスがデフォルトのグローバル ポリシーで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。このマップは **global_policy** と呼ばれ、デフォルトの検査トラフィックで検査を実行します。適用できるグローバル ポリシーは 1 つのみです。このため、グローバル ポリシーの内容を変更する場合は、デフォルトのポリシーを編集するか、ディセーブルにして新しいものを適用する必要があります。

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ています。

```
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

次に、接続ポリシーに対する **policy-map** コマンドの例を示します。ここでは、Web サーバ 10.1.1.1 にアクセスできる接続の数を制限しています。

```
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
```

次の例では、ポリシー マップで複数一致がどのように機能するかを示しています。

```
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
```

次の例では、使用可能な最初のクラス マップにトラフィックが一致し、同じ機能ドメインのアクションを指定している以降のどのクラス マップにも一致しない様子を示しています。

```
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 接続が開始されると、**class telnet_traffic** と照合されます。同様に、FTP 接続が開始されると、**class ftp_traffic** と照合されます。Telnet と FTP 以外の TCP 接続の場合は、**class tcp_traffic** と照合されます。Telnet または FTP 接続が **class tcp_traffic** と一致する可能性があったとしても、すでに他のクラスと一致しているので、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 マップに含めるクラス 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** コマンドで使用中の場合、このポリシー 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 1 つのインターフェイスに割り当てるか、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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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検査アプリケーション トラフィックの特殊アクションを定義します。検査ポリシー マップの指定を削除するには、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*

シンタックスの説明

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。指定できるタイプは、次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **radius-accounting** • **sip** • **skinny** • **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るので、使用できません。すべてのタイプのポリシー マップが同じネーム スペースを使用しているため、他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
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 フレームワークを利用すると、数多くのアプリケーション検査のための特別なアクションを設定できます。**inspect** コマンドを使用して、レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で検査エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成した検査ポリシー マップで定義するアクションを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、検査ポリシー マップの名前です。

検査ポリシー マップは、ポリシー マップ コンフィギュレーション モードに入力された次のコマンドのうち 1 つまたは複数のコマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。

- **match** コマンド：**match** コマンドを直接検査ポリシー マップに定義できます。そうすることで、アプリケーション トラフィックを、URL 文字列などのこのアプリケーションに特有の基準と照合します。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。使用可能な **match** コマンドは、アプリケーションにより異なります。
- **class** コマンド：このコマンドは、ポリシー マップで検査クラス マップを特定します（検査クラス マップを作成する **class-map type inspect** コマンドを参照）。検査クラス マップには、URL 文字列などの、アプリケーション特有の基準によってアプリケーションのトラフィックを照合する複数の **match** コマンドが含まれます。それに応じて、ポリシー マップでアクションをイネーブルにします。クラス マップを作成することと、検査ポリシー マップに直接 **match** コマンドを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 マップを再利用できることです。
- **parameters** コマンド：パラメータは、検査エンジンの動作に影響を与えます。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に一致する正規表現を指定できます。複数の正規表現をグループ化する方法については、**regex** コマンドと **class-map type regex** コマンドを参照してください。

デフォルトの検査ポリシー マップ コンフィギュレーションには、DNS パケットのメッセージの最大長を 512 バイトに設定する次のコマンドが含まれます。

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

1 つのパケットで複数の異なる **match** コマンドまたは **class** コマンドが一致する場合、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番はセキュリティ アプライアンスの内部規則で決定されます。ポリシー マップに追加される順番ではありません。内部規則は、アプリケーションのタイプと、パケット解析の論理的な進行状況によって決定されます。ユーザは設定できません。たとえば、HTTP トラフィックの場合、Request Method フィールドは Header Host Length フィールドよりも先に解析されます。Request Method フィールドのアクションは Header Host Length フィールドのアクションの前に実行されます。たとえば、次の match コマンドは任意の順番で入力できますが、**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
```

あるアクションがパケットをドロップすると、他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は、それ以降のどの **match** コマンドも照合されません。最初のアクションがパケットのロギングである場合は、接続のリセットなどの 2 番目のアクションが発生する可能性があります（同じ **match** コマンドに対して、**reset**（または **drop-connection** など）と **log** アクションを両方設定でできます。その場合、パケットは、指定の照合についてリセットされる前に記録されます）。

パケットが同一の複数の **match** コマンドまたは **class** コマンドと一致する場合、ポリシー マップに出現する順番で一致します。たとえば、ヘッダーの長さが 1001 のパケットの場合、その下にある最初のコマンドに一致し、記録され、次に 2 番目のコマンドと一致し、リセットされます。この 2 つの **match** コマンドの順番を逆にした場合、パケットはドロップされ、接続が 2 番目の **match** コマンドと一致する前にリセットされます。このパケットは記録されません。

```
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
```

あるクラス マップが別のクラス マップ、またはクラス マップ内で優先度の最も低い **match** コマンドに基づいた **match** コマンドと同じタイプであると判断されます（優先度は内部規則に基づきます）。クラス マップが他のクラス マップと同じ優先度の最も低いタイプの **match** コマンドである場合、このクラス マップはポリシー マップに追加される順番に従って照合されます。各クラス マップの優先度の最も低いコマンドが異なる場合、優先度の高い **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

次に、HTTP 検査ポリシー マップと関連するクラス マップの例を示します。このポリシー マップは、サービス ポリシーによってイネーブルになるレイヤ 3/4 ポリシー マップにより有効になります。

```
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 マップに含めるクラス 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検査クラス マップを作成します。
parameters	検査ポリシー マップのパラメータ コンフィギュレーション モードに入ります。
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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

policy-server-secret

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鍵を設定するには、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。これは CA SiteMinder コマンドによる SSO です。

秘密鍵を削除するには、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）　SSO 認証にはこのコマンドが必要です。

シンタックスの説明

secret-key	認証の通信内容を暗号化するための秘密鍵として使用される文字列。最小文字数にも最大文字数にも制限はありません。

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
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 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。最初に **sso-server** コマンドを使用して SSO サーバを作成します。次に、**policy-server-secret** コマンドを使用することにより、セキュリティ アプライアンスと SSO サーバ間の認証通信が保証されます。

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。秘密鍵は、セキュリティ アプライアンスでは `policy-server-secret` コマンドを使用して設定され、SiteMinder Policy Server では Cisco Java プラグイン認証スキームを使用して設定されます。

現在、セキュリティ アプライアンスは、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）をサポートしています。

例

次のコマンドは、webvpn-sso-siteminder コンフィギュレーション モードで入力され、ランダムな文字列を引数として含んでいます。このコマンドにより、SSO サーバの認証通信用の秘密鍵が作成されます。

```
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	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作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 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 インターフェイスのポーリング時間と待機時間を指定するには、フェールオーバー 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*]

シンタックスの説明

holdtime *time*	(オプション)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期限を設定します。この期限が経過すると、ピア インターフェイスは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 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	（オプション）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
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)	オプションの ***holdtime*** *time* 値が追加され、ポーリング時間をミリ秒で指定できるように変更されました。

使用上のガイドライン

polltime interface コマンドを使用して、指定したフェールオーバー グループに関連付けられたインターフェイスで hello パケットが送信される周波数を変更します。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。**failover polltime interface** コマンドは、Active/Standby フェールオーバー コンフィギュレーションで使用します。

装置のポーリング時間の 5 倍未満の ***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、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。インターフェイスのテストが開始されるのは、待機期間の半分が経過したときに、インターフェイス上で hello パケットが受信されていない場合です。

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 アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー待機時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、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 を使用して再登録する必要があります。

例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。フェールオーバー グループ 1 のデータ インターフェイスに対して、インターフェイス ポーリング時間は 500 ミリ秒、待機時間は 5 秒に設定されます。

```
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 ポーリング期間と待機期間を指定します。
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待機期間を指定します。

pop3s

POP3S コンフィギュレーション モードに入るには、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、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。受信者（または受信者のクライアント電子メール レシーバー）は、サーバ上のメールボックスを定期的に確認し、電子メールがあればダウンロードします。この標準プロトコルは、一般的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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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。

例

次の例は、POP3S コンフィギュレーション モードに入る方法を示しています。

```
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 プロキシがリッスンするポートを指定するには、適切な電子メール プロキシ 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

シンタックスの説明

portnum	電子メール プロキシが使用するポート。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
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(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

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

次の例は、IMAP4S 電子メール プロキシのポートを 1066 に設定する方法を示しています。

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

port-forward

転送 TCP ポートを介して WebVPN ユーザがアクセスできるアプリケーションのセットを設定するには、グローバル コンフィギュレーション モードで **port-forward** コマンドを使用します。複数のアプリケーションへのアクセスを設定するには、このコマンドを同じ listname で複数回（アプリケーションごとに 1 回）使用します。設定したリスト全体を削除するには、**no port-forward** *listname* コマンドを使用します。設定したアプリケーションを削除するには、**no port-forward** *listname localport* コマンドを使用します（*remoteserver* パラメータおよび *remoteport* パラメータは含める必要はありません）。

port-forward {*listname localport remoteserver remoteport description*}

no port-forward *listname*

no port-forward *listname localport*

シンタックスの説明

description	エンド ユーザのポート転送 Java アプレット画面に表示する、アプリケーション名または簡単な説明を入力します。最大 64 文字です。
listname	WebVPN ユーザがアクセスできるアプリケーション（転送 TCP ポート）のセットをグループ化します。最大 64 文字です。
localport	アプリケーションの TCP トラフィックをリッスンするローカル ポートを指定します。ローカル ポート番号は、1 つの *listname* に対して一度だけ使用できます。
remoteport	このアプリケーションが接続するリモート サーバ上のポートを指定します。
remoteserver	リモート サーバの DNS 名または IP アドレスをアプリケーション用に入力します。DNS 名を使用することをお勧めします。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

デフォルト

デフォルトのポート転送リストはありません。

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
グローバル 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(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

特定の TCP ポート転送アプリケーションへのアクセスを特定のユーザまたはグループ ポリシーに許可するには、webvpn モードで、ここで作成した *listname* を **port-forward** コマンドと共に使用します。

例

次の例は、IMAP4S 電子メール、SMTPS 電子メール、DDTS、および Telnet へのアクセスを提供する *SalesGroupPorts* というポート転送リストを作成する方法を示しています。次の表に、この例で使用されている、各アプリケーションの値を示します。

アプリケーション	ローカル ポート	サーバ DNS 名	リモート ポート	説明
IMAP4S 電子メール	143	IMAP4Sserver	20143	Get Mail
SMTPS 電子メール	25	SMTPSserver	20025	Send Mail
DDTS over SSH	22	DDTSserver	20022	DDTS over SSH
Telnet	23	Telnetserver	20023	Telnet

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

関連コマンド

コマンド	説明
clear configuration port-forward [*listname*]	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドだけを削除します。
port-forward	ユーザまたはグループ ポリシーの WebVPN アプリケーション アクセスをイネーブルにするには、webvpn モードでこのコマンドを使用します。
show running-config port-forward	現在設定されている **port-forward** コマンドのセットを表示します。
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 モードに入って、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 コンフィギュレーション値を設定できます。

port-forward（webvpn）

WebVPN アプリケーション アクセスをこのユーザまたはグループ ポリシーに対してイネーブルにするには、webvpn モードで **port-forward** コマンドを使用します。このモードには、グループ ポリシー モードまたはユーザ名モードから入ります。**port-forward none** コマンドを発行することで作成されたヌル値を含む、ポート転送アトリビュー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** 形式を使用します。**no** オプションを使用すると、リストを別のグループ ポリシーから継承できます。ポート転送リストを継承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 {**value** *listname* | **none**}

no port-forward

シンタックスの説明

none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
value listname	WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。リストを定義するには、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。

デフォルト

デフォルトでは、ポート転送はディセーブルになっています。

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
WebVPN モード	•	—	•	—	—

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

コマンドを 2 回使用すると、先行する設定値が上書きされます。

webvpn モードで **port-forward** コマンドを使用してアプリケーション アクセスをイネーブルにする前に、WebVPN 接続で使用することをユーザに許可するアプリケーションのリストを定義する必要があります。このリストを定義するには、グローバル 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。

例

次の例は、*ports1* というポート転送リストを FirstGroup というグループ ポリシーに対して設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
```

関連コマンド

コマンド	説明
clear configuration port-forward [*listname*]	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドだけを削除します。
port-forward	WebVPN ユーザがアクセスできるアプリケーション（転送ポート）を定義するには、コンフィギュレーション モードでこのコマンドを使用します。
show running-config port-forward	現在設定されている **port-forward** コマンドのセットを表示します。
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 モードに入って、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 コンフィギュレーション値を設定できます。

port-forward-name

エンド ユーザが TCP ポート転送を識別できる表示名を、特定のユーザまたはグループ ポリシーに対して設定するには、webvpn モードで **port-forward-name** コマンドを使用します。このモードには、グループ ポリシー モードまたはユーザ名モードから入ります。**port-forward-name none** コマンドを使用することにより作成されたヌル値を含む表示名を削除するには、このコマンドの no 形式を使用します。**no** オプションを指定すると、デフォルト名の「Application Access」が復元されます。表示名を復元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

シンタックスの説明

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。値を継承しないようにします。
value *name*	エンド ユーザに対してポート転送を説明します。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
Webvpn	•	—	•	—	—

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

次の例は、「Remote Access TCP Applications」という名前を FirstGroup というグループ ポリシーに対して設定する方法を示しています。

```
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 モードに入って、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 コンフィギュレーション値を設定できます。

port-object

ポート オブジェクトをサービス オブジェクト グループに追加するには、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*

シンタックスの説明

begin_service	サービス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 で指定する必要があります。
end_service	サービス範囲の終了値である、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 で指定する必要があります。
eq service	サービス オブジェクトに 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。
range	ポートの範囲（包含）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
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のものです。

使用上のガイドライン

特定のサービス（ポート）またはサービス範囲（複数のポート）のいずれかのオブジェクトを定義するには、サービス コンフィギュレーション モードで **object-group** と共に **port-object** コマンドを使用します。

TCP サービスまたは UDP サービスの名前を指定する場合、その名前は、TCP、UDP、またはその両方でサポートされている名前のいずれかで、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、tcp、udp、tcp-udp の各プロトコル タイプの場合、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、TCP および UDP の有効な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。

表 22-2

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

次の例は、サービス コンフィギュレーション モードで **port-object** コマンドを使用して、新しいポート（サービス）オブジェクト グループを作成する方法を示しています。

```
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。

pppoe client route distance

PPPoE を通してラーニングされたルータの管理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*

シンタックスの説明

distance	PPPoE を通してラーニングされたルータに適用する管理ディスタンスです。有効な値は 1 ～ 255 です。

デフォルト

PPPoE を通してラーニングされたルータに指定されているデフォルトの管理ディスタンスは 1 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
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 client route distance コマンドは、ルータが PPPoE からラーニングされた場合にのみチェックされます。ルータが PPPoE からラーニングされた後に **pppoe client route distance** コマンドが入力された場合、指定の管理ディスタンスは既存のラーニングされたルートに対して有効でなくなります。指定した管理ディスタンスが与えられるのは、このコマンドの入力後にラーニングされたルートだけです。

PPPoE を利用して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優先順位を指定する必要があります。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 トラッキングでのみサポートされます。

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

次の例では、GigabitEthernet0/2 上で PPPoE を利用してデフォルト ルートを取得しています。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 オペレーションによって、外部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監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で PPPoE を通じて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 を通じて取得した 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 を通じてラーニングしたルートを、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 監視オペレーションを定義します。
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ク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

シンタックスの説明

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
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 client route track のチェックは、ルートを PPPoE からラーニングした場合にのみ行われます。PPPoE を通じてルートをラーニングした後に **pppoe client route track** コマンドを入力した場合、ラーニングした既存のルートは、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ラーニングされたルートだけです。

PPPoE を利用して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優先順位を指定する必要があります。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 トラッキングでのみサポートされます。

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

次の例では、GigabitEthernet0/2 上で PPPoE を利用してデフォルト ルートを取得しています。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 オペレーションによって、外部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監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で PPPoE を通じて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 を通じて取得した 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 を通じてラーニングしたルートに管理ディスタンスを割り当てます。
sla monitor	SLA 監視オペレーションを定義します。
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ク済みの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

シンタックスの説明

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
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 client secondary コマンドは、PPPoE セッションの起動時にのみチェックされます。PPPoE を通じてルートをラーニングした後に **pppoe client route track** コマンドを入力した場合、ラーニングした既存のルートは、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ラーニングされたルートだけです。

PPPoE を利用して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優先順位を指定する必要があります。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 トラッキングでのみサポートされます。

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

次の例では、GigabitEthernet0/2 上で PPPoE を利用してデフォルト ルートを取得しています。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 オペレーションによって、外部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監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で PPPoE を通じて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 を通じて取得した 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 を通じてラーニングしたルートに管理ディスタンスを割り当てます。
pppoe client route track	PPPoE を通じてラーニングしたルートを、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 監視オペレーションを定義します。

preempt

装置の優先順位が高い場合に、その装置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*]

シンタックスの説明

delay	ピアがプリエンプションされるまでの待ち時間（秒）。有効な値は 1 ～ 1200 秒です。

デフォルト

デフォルトでは、待ち時間はありません。

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
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優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ただし、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。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上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** コマンドを使用して設定されている場合、そのフェールオーバー グループは、指定装置上で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、フェールオーバー グループが現在アクティブである装置から接続が複製されるまで、プリエンプションは実行されません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちらのフェールオーバー グループも、**preempt** コマンドを使用して待ち時間 100 秒で設定されています。したがって、これらのグループは、優先する装置が利用可能になってから 100 秒後に、その装置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。
primary	設定しているフェールオーバー グループのフェールオーバー ペア優先順位における、プライマリ装置を指定します。
secondary	設定しているフェールオーバー グループのフェールオーバー ペア優先順位における、セカンダリ装置を指定します。

prefix-list

ABR タイプ 3 LSA フィルタリングのプレフィックス リストの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 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*]

シンタックスの説明

/	*network* 値と *len* 値の間に必要な区切り記号。
deny	一致した条件へのアクセスを拒否します。
ge *min_value*	（オプション）一致する必要のある最小プレフィックス長を指定します。*min_value* 引数の値は、*len* 引数の値より大きくする必要があります。また、*max_value* 引数が存在する場合は、それ以下にする必要があります。
le *max_value*	（オプション）一致する必要のある最大プレフィックス長を指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合は、その値以上にする必要があり、*min_value* 引数が存在しない場合は、*len* 引数の値より大きく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*	（オプション）指定したシーケンス番号を、作成中のプレフィックス リストに適用します。

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 リストの最初のエントリにシーケンス番号 5 が割り当てられ、以降の各エントリには、5 ずつ増加するシーケンス番号が割り当てられます。

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
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のものです。

使用上のガイドライン

prefix-list コマンドは、ABR タイプ 3 LSA フィルタリング コマンドです。ABR タイプ 3 LSA フィルタリングによって OSPF 実行中の ABR 機能を拡張し、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だけが一方から他方のエリアに送信されます。その他のプレフィックスは、すべてそれぞれの 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 エリアが終点または起点となるトラフィック、あるいはそのエリアの着信および発信両方のトラフィックに適用できます。

プレフィックス リストの複数のエントリが所定のプレフィックスに一致する場合、最も小さいシーケンス番号を持つエントリが使用されます。セキュリティ アプライアンスは、プレフィックス リストの最上部から、つまり最も小さいシーケンス番号を持つ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。それらは、**no prefix-list sequence-number** コマンドで抑制できます。シーケンス番号は、5 ずつ増分されます。プレフィックス リスト内に最初に生成されるシーケンス番号は 5 です。リスト内の次のエントリのシーケンス番号は 10 となり、以降も同様となります。あるエントリの値を指定し、後続のエントリの値を指定しない場合、生成されるシーケンス番号は、指定した値から 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* 引数より具体的なプレフィックスと一致する必要のあるプレフィックスの長さの範囲を指定できます。***ge*** キーワードも ***le*** キーワードも指定しない場合は、完全一致が前提とされます。***ge*** キーワードだけを指定した場合の範囲は、*min_value* ～ 32 です。***le*** キーワードだけを指定した場合の範囲は、*len* ～ *max_value* です。

min_value 引数および *max_value* 引数の値は、次の条件を満たしている必要があります。

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

特定のエントリをプレフィックス リストから削除するには、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、関連付けられた **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

次の例では、デフォルト ルート 0.0.0.0/0 を拒否します。

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

次の例では、プレフィックス 10.0.0.0/8 を許可します。

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

次の例は、プレフィックス 192/8 を持つルートで最大 24 ビットのマスク長を受け入れる方法を示しています。

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

次の例は、プレフィックス 192/8 を持つルートで 25 ビットより大きいマスク長を拒否する方法を示しています。

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

次の例は、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方法を示しています。

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

次の例は、すべてのアドレス空間で 25 ビットより大きいマスク長を拒否する方法を示しています。

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

次の例は、プレフィックス 10/8 を持つすべてのルートを拒否する方法を示しています。

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

次の例は、プレフィックス 192.168.1/24 を持つルートで長さが 25 ビットより大きいすべてのマスクを拒否する方法を示しています。

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

次の例は、プレフィックス 0/0 を持つすべてのルートを許可する方法を示しています。

```
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*]

シンタックスの説明

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。最大で 80 文字入力できます。

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
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のものです。

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。つまり、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、コンフィギュレーション内で常に、関連付けられたプレフィックス リストの前の行に記述されます。これは、コマンドを入力した順序とは関係ありません。

すでに説明があるプレフィックス 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、元の説明は新しい説明に置き換えられます。

このコマンドの **no** 形式を使用している場合、テキスト説明を入力する必要はありません。

例

次の例では、MyPrefixList という名前のプレフィックス リストの説明を追加します。**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すでに追加されているものの、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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になっています。

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
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のものです。

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にある場合、シーケンス番号は、手動で設定したものも含めて、コンフィギュレーションの **prefix-list** コマンドから削除されます。また、新しいプレフィックス リスト エントリには、シーケンス番号が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、すべてのプレフィックス リスト エントリには、デフォルトの番号付け方式（開始値は 5 で、各番号は 5 ずつ増分される）で、シーケンス番号が割り当てられます。番号付けをディセーブルにする前に、シーケンス番号を手動でプレフィックス リスト エントリに割り当てた場合、手動で割り当てた番号が復元されます。自動番号付けがディセーブルになっている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、それらのシーケンス番号は表示されません。

例

次の例では、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

事前共有キーに基づく IKE 接続をサポートするために事前共有キーを指定するには、トンネル グループ ipsec アトリビュート 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

シンタックスの説明

key	1 ～ 128 文字の英数字でキーを指定します。

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
トンネル グループ ipsec アトリビュート 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(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

このアトリビュートは、すべての IPSec トンネル グループ タイプに適用できます。

例

config-ipsec コンフィギュレーション モードで入力された次のコマンドは、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ため、事前共有キー XYZX を指定します。

```
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 グループを消去します。
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 アトリビュートを設定します。

primary

フェールオーバー グループに対するプライマリ装置の優先順位を高くするには、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

フェールオーバー グループに対して **primary** または **secondary** を指定しない場合、そのフェールオーバー グループは、デフォルトでは **primary** に設定されます。

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
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優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。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。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちら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、優先する装置が使用可能になったときにその装置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	優先する装置が使用可能になったときに、フェールオーバー グループをその装置上で強制的にアクティブにします。
secondary	セカンダリ装置に、プライマリ装置より高い優先順位を設定します。

priority

厳密なスケジューリング優先順位をこのクラスに適用するには、クラス モードで **priority** コマンドを使用します。優先順位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

シンタックスの説明

このコマンドには、パラメータも変数もありません。

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

priority コマンドを発行するには、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。

例

次に、ポリシー マップ モードの **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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

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 デバイスの優先順位を設定するには、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。デフォルトの優先順位指定に戻すには、このコマンドの **no** 形式を使用します。

priority *priority*

no priority

シンタックスの説明

priority	このデバイスに割り当てる優先順位（範囲は 1 ～ 10）。

デフォルト

デフォルトの優先順位は、デバイスのモデル番号によって異なります。

モデル番号	デフォルトの優先順位
5520	5
5540	7

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
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 モードに入る必要があります。

このコマンドは、仮想ロードバランシング クラスタに参加しているローカル デバイスの優先順位を設定します。

優先順位は、1（最低）～ 10（最高）の整数である必要があります。

優先順位は、マスター選定プロセスで、VPN ロードバランシング クラスタ内のどのデバイスがそのクラスタのマスター デバイスまたはプライマリ デバイスになるかを決定する方法の 1 つとして使用されます。マスター選定プロセスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

このコマンドの ***no*** 形式を使用すると、優先順位指定がデフォルト値に戻ります。

例

次に、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。これには、現在のデバイスの優先順位を 9 に設定する **priority** コマンドが含まれています。

```
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 モードに入ります。

priority-queue

インターフェイス上にプライオリティ キューイングを設定するには、グローバル コンフィギュレーション モードで priority-queue コマンドを使用します。この指定を削除するには、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*

シンタックスの説明

interface-name	プライオリティ キューイング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。

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になっています。

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
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 アプライアンスでは、次の 2 つのトラフィック クラスを使用できます。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティ キューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングが発生するようにするには、名前付き物理インターフェイスに対してプライオリティ キューを作成する必要があります。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。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義された各物理インターフェイスに対して適用できます。**priority-queue** コマンドは、VLAN インターフェイスには適用できません。

priority-queue コマンドを使用すると、プライオリティ キュー モードに入ります。モードはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

指定する tx-ring-limit 値および queue-limit 値は、優先順位の高い低遅延キューとベストエフォートキューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

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。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリの量を超えることはできません。理論上の最大パケット数は、2,147,483,647（つまり、全二重時の回線速度が上限）です。

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

例

次の例では、test というインターフェイスのプライオリティ キューを設定して、キューの上限を 30,000 パケット、送信キューの上限を 256 パケットと指定しています。

```
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いつでも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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
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、現在のすべてのプライオリティ キュー、および queue-limit と tx-ring-limit のコンフィギュレーション値が表示されます。

privilege

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。この設定を取り消すには、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*

シンタックスの説明

clear	（オプション）指定されたコマンドに対応する **clear** コマンドの特権レベルを設定します。
command *command*	特権レベルを設定する対象のコマンドを指定します。
configure	（オプション）指定したコマンドの特権レベルを設定します。
level *level*	特権レベルを指定します。有効値は 0 ～ 15 です。
mode enable	（オプション）コマンドのイネーブル モード用のレベルであることを指定します。
mode configure	（オプション）コマンドの設定モード用のレベルであることを指定します。
show	指定されたコマンドに対応する **show** コマンドの特権レベルを設定します。

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
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のものです。

使用上のガイドライン

privilege コマンドを使用すると、セキュリティ アプライアンスのコマンドにユーザ定義の特権レベルを設定できます。このコマンドは、**show** コマンド、および **clear** コマンドという関連するコンフィギュレーションに異なる特権レベルを設定する場合に特に役立ちます。新しい特権レベルを使用する前に、セキュリティ ポリシーでコマンドの特権レベル変更を必ず検証してください。

コマンドおよびユーザに特権レベルが設定されている場合、両者は比較されて指定ユーザが指定コマンドを実行できるかどうかが判別されます。ユーザの特権レベルがコマンドの特権レベルよりも低い場合、ユーザはそのコマンドを実行できません。

特権レベルを切り替えるには、**login** コマンドを使用して別の特権レベルにアクセスし、適切な **logout** コマンド、**exit** コマンド、または **quit** コマンドを使用してそのレベルを終了します。

mode enable キーワードおよび **mode configure** キーワードは、イネーブル モードと設定モードの両方を持つコマンドで使用します。

特権レベルの数字が小さいほど、レベルは低くなります。

（注）　**aaa authentication** コマンドと **aaa authorization** コマンドには、AAA サーバのコンフィギュレーションで使用する前に、定義する新しい特権レベルを入れる必要があります。

例

次の例は、個々のユーザに特権レベル「5」を設定する方法を示しています。

```
username intern1 password pass1 privilege 5
```

次の例は、特権レベル「5」の **show** コマンド セットを定義する方法を示しています。

```
hostname(config)# privilege show level 5 command alias
hostname(config)# privilege show level 5 command apply
hostname(config)# privilege show level 5 command arp
hostname(config)# privilege show level 5 command auth-prompt
hostname(config)# privilege show level 5 command blocks
hostname(config)#
```

次の例は、特権レベル 11 を AAA 許可コンフィギュレーション全体に適用する方法を示しています。

```
hostname(config)# privilege configure level 11 command aaa
hostname(config)# privilege configure level 11 command aaa-server
hostname(config)# privilege configure level 11 command access-group
hostname(config)# privilege configure level 11 command access-list
hostname(config)# privilege configure level 11 command activation-key
hostname(config)# privilege configure level 11 command age
hostname(config)# privilege configure level 11 command alias
hostname(config)# privilege configure level 11 command apply
hostname(config)#
```

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 コマンド文を削除します。
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

セッション プロンプト表示を設定するには、コンフィギュレーション モード（P_CONF）、複製（P_REP）、シングル モード、およびマルチモードのシステム コンテキストで **prompt** コマンドを使用します。設定されたプロンプトを表示できるのは、管理者だけです。ユーザ コンテキストでは、デフォルトのホスト名 / コンテキスト（コンフィギュレーション モード）プロンプトが表示されます。

prompt [*<keyword>* [*keyword>*] ...]

no prompt

シンタックスの説明

キーワード	説明
context	現在のコンテキストを表示するプロンプトを設定します（マルチモードのみ）。
domain	ドメインを表示するプロンプトを設定します。
hostname	ホスト名を表示するプロンプトを設定します。
priority	「failover lan unit」設定を表示するプロンプトを設定します。
state	現在のトラフィック処理の状態を表示するプロンプトを設定します。 *state* キーワードに対しては、次の値が表示されます。 *act*：装置は、トラフィックが通過している状態です（フェールオーバーがイネーブルになっている Active など）。 *stby*：装置は、トラフィックが通過している状態ではなく、スタンバイ、障害、またはその他の非アクティブ状態になっている可能性があります。 *actNoFailover*：装置は、非フェールオーバーで、トラフィックが通過できる状態です。

デフォルト

デフォルトはホスト名 / コンテキスト プロンプトです。

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
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

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モジュールにログインしているかを一目で判別できます。この機能は、フェールオーバーの発生時、2 つのモジュールのホスト名が同じ場合に重要になります。

例

次の例は、プロンプトを設定する方法を示しています。

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

前提条件は次のとおりです。

```
hostname = myasa
context = admin
priority = failover lan unit primary
state = Active (with failover enabled)
```

プロンプトは次のように表示されます。

```
myasa/admin/pri/act>
myasa/admin/pri/act#
myasa/admin/pri/act(config)#
myasa/admin/pri/act(config-interface)#
```

ヘルプと使用方法は次のとおりです。

```
asa# help prompt

asa# prompt ?

configure mode commands/options:
hostname    Configures the prompt to display the hostname
domain       Configures the prompt to display the domain
context       Configures the prompt to display the current context (multimode only)
priority       Configures the prompt to display the 'failover lan unit' setting
state           Configures the prompt to display the current traffic handling state
```

関連コマンド

コマンド	説明
clear config prompt	設定されているプロンプトを消去します。
no prompt	プロンプトを完全に削除します。
show running-config prompt	設定されているプロンプトを表示します。

protocol-enforcement

圧縮およびループ ポインタ チェックを含む、ドメイン名、ラベルの長さ、形式のチェック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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

プロトコル強制はデフォルトでイネーブルになっています。このコマンドは、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定している場合は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** を設定していない場合、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
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

特定の条件下では、このコマンドがディセーブルであってもプロトコル強制は行われます。たとえば、DNS リソース レコードの分類、NAT または TSIG チェックなど、DNS リソース レコードの解析が他の目的に必要な場合に行われます。

例

次の例では、プロトコル強制を DNS 検査ポリシー マップ内で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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

protocol http

CRL を取得するために許可する配布ポイント 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。アクセス権があれば、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、HTTP を許可する設定になっています。

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(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

このコマンドを使用する場合は、HTTP ルールを公開インターフェイス フィルタに必ず割り当ててください。

例

次の例では、ca-crl コンフィギュレーション モードに入り、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 を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
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。アクセス権があれば、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、LDAP を許可する設定になっています。

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

次の例では、ca-crl コンフィギュレーション モードに入り、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 を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol http	HTTP を CRL 取得方法として指定します。
protocol scep	SCEP を CRL 取得方法として指定します。

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 設定モードで **protocol scep** コマンドを使用します。アクセス権があれば、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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、SCEP を許可する設定になっています。

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

次の例では、ca-crl コンフィギュレーション モードに入り、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 モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol http	HTTP を CRL 取得方法として指定します。
protocol ldap	LDAP を CRL 取得方法として指定します。

protocol-object

プロトコル オブジェクトをプロトコル オブジェクト グループに追加するには、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*

シンタックスの説明

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
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のものです。

使用上のガイドライン

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するには、**object-group** コマンドと共に **protocol-object** コマンドを使用します。

protocol 引数を使用して、IP プロトコルの名前または番号を指定できます。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

次の例は、プロトコル オブジェクトを定義する方法を示しています。

```
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

プロトコル違反に対する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]

no protocol-violation action [drop | log]

シンタックスの説明

このコマンドには、引数もキーワードもありません。

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
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。

例

次の例では、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方法を示します。

```
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 マップに含めるクラス 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検査クラス 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	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

proxy-bypass

コンテンツの最低限の書き換えを実行すると共に、書き換えるコンテンツのタイプとして、外部リンクと XML の両方またはいずれか一方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 モードで **proxy-bypass** コマンドを使用します。プロキシ 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}]**

シンタックスの説明

host	トラフィックの転送先となるホストを指定します。ホスト IP アドレスまたはホスト名のいずれかを使用してください。
interface	プロキシ バイパス用の ASA インターフェイスを特定します。
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	一致させるパターンを指定します。
path-mask	正規表現を含むことができるパターンと一致するよう、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。 * ：すべてと一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列と共に使用する必要があります。 ? ：任意の 1 文字と一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 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特定します。
port number	プロキシ バイパス用に予約されている上位番号のポートを指定します。ポートの範囲は 20000 ～ -21000 です。1 つのプロキシ バイパスの規則に対してポートは 1 つだけ使用できます。
rewrite	（オプション）書き換えに対する追加規則を指定します（none、または XML と link の組み合せを付加）。
target	トラフィックの転送先となるリモート サーバを特定します。
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。ポートは、特に指定しない限り、HTTP の場合は 80、HTTPS の場合は 443 です。
xml	XML コンテンツの書き換えを指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

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。プロキシ バイパス コマンドにより、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が決定されます。

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ありません。プロキシ バイパス規則は、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って一意に特定されます。

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、これらのポートのセキュリティ アプライアンスへのアクセスを許可するためにファイアウォール設定の変更が必要になることがあります。このような制限を回避するには、パス マスクを使用してください。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。

パスとは、URL の .com または .org あるいはその他のタイプのドメイン名の後にあるものすべてをいいます。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスです。同様に、www.mycompany.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての「hr」サイトにプロキシ バイパスを使用する場合は、/hr* というようにワイルドカード * を使用すると、コマンドを複数回使用しないようにできます。

例

次の例は、HTTP とそのデフォルト ポート 80 を使用するセキュリティ アプライアンスが webvpn インターフェイス上でプロキシ　バイパス用のポート　20001　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るように設定する方法を示しています。

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

次の例は、HTTPS とそのデフォルト ポート 443 を使用するセキュリティ アプライアンスが外部インターフェイスのプロキシ バイパス用パス マスク「mypath/*」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るように設定する方法を示しています。

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

関連コマンド -

コマンド	説明
apcf	特定のアプリケーションに使用する非標準の規則を指定します。
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。

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

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトは、ルート ディレクトリ（/）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
特権 EXEC	•	•	•	—	•

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、機能の点で ***dir*** コマンドと類似しています。

例　次の例は、現在の作業ディレクトリを表示する方法を示しています。

```
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移動します。
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。