CHAPTER 32

tcp-map コマンド～ type echo コマンド

tcp-map

一連の TCP 正規化アクションを定義するには、グローバル コンフィギュレーション モードで **tcp-map** コマンドを使用します。TCP 正規化機能によって、異常なパケットを識別する基準を指定できます。セキュリティ アプライアンスは、異常なパケットが検出されるとそれらをドロップします。TCP 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。

tcp-map *map_name*

no tcp-map *map_name*

構文の説明

map_name	TCP マップ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

この機能は モジュラ ポリシー フレームワーク を使用します。最初に、**tcp-map** コマンドを使用して実行する TCP 正規化アクションを定義します。**tcp-map** コマンドによって、tcp マップ コンフィギュレーション モードが開始されます。このモードで、1 つ以上のコマンドを入力して、TCP 正規化アクションを定義できます。その後、**class-map** コマンドを使用して、TCP マップを適用するトラフィックを定義します。**policy-map** コマンドを入力してポリシーを定義し、**class** コマンドを入力してクラスマップを参照します。クラス コンフィギュレーション モードで、**set connection advanced-options** コマンドを入力して TCP マップを参照します。最後に、**service-policy** コマンドを使用して、インターフェイスにポリシー マップを適用します。モジュラ ポリシー フレームワークの仕組みの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

次のコマンドは、tcp マップ コンフィギュレーション モードで使用可能です。

check-retransmission	再送信データのチェックをイネーブルまたはディセーブルにします。
checksum-verification	チェックサムの検証をイネーブルまたはディセーブルにします。
exceed-mss	ピアによって設定された MSS を超えるパケットを許可またはドロップします。

queue-limit	TCP 接続のキューに入れることができる順序が不正なパケットの最大数を設定します。このコマンドは、ASA 5500 シリーズセキュリティ アプライアンスでのみ使用可能です。PIX 500 シリーズセキュリティ アプライアンスではキュー制限は 3 で、この値は変更できません。
reserved-bits	セキュリティ アプライアンスに予約済みフラグ ポリシーを設定します。
syn-data	データを持つ SYN パケットを許可またはドロップします。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。
ttl-evasion-protection	セキュリティ アプライアンスによって提供された TTL 回避保護をイネーブルまたはディセーブルにします。
urgent-flag	セキュリティ アプライアンスを通じて URG ポインタを許可またはクリアします。
window-variation	予期せずウィンドウ サイズが変更された接続をドロップします。

例

たとえば、既知の FTP データ ポートと Telnet ポートの間の TCP ポート範囲に送信されるすべてのトラフィックで緊急フラグと緊急オフセット パケットを許可するには、次のコマンドを入力します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow

hostname(config-tcp-map)# class-map urg-class
hostname(config-cmap)# match port tcp range ftp-data telnet

hostname(config-cmap)# policy-map pmap
hostname(config-pmap)# class urg-class
hostname(config-pmap-c)# set connection advanced-options tmap

hostname(config-pmap-c)# service-policy pmap global
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィック分類に使用するクラス マップを指定します。
clear configure tcp-map	TCP マップのコンフィギュレーションをクリアします。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。

tcp-options

セキュリティ アプライアンスを通じて TCP オプションを許可またはクリアするには、tcp マップ コンフィギュレーション モードで **tcp-options** 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。

tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

no tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

tcp-options range *lower upper* {**allow** | **clear** | **drop**}

no tcp-options range *lower upper* {**allow** | **clear** | **drop**}

構文の説明

allow	TCP ノーマライザを介して TCP オプションを許可します。
clear	TCP ノーマライザを介して TCP オプションをクリアし、パケットを許可します。
drop	パケットをドロップします。
lower	下位バインド範囲（6 ～ 7）および（9 ～ 255）。
selective-ack	選択的確認応答メカニズム（SACK）オプションを設定します。デフォルトでは、SACK オプションを許可します。
timestamp	タイムスタンプ オプションを設定します。タイムスタンプ オプションをクリアすると、PAWS と RTT がディセーブルになります。デフォルトでは、タイムスタンプ オプションを許可します。
upper	上位バインド範囲（6 ～ 7）および（9 ～ 255）。
window-scale	ウィンドウ スケール メカニズム オプションを設定します。デフォルトでは、ウィンドウ スケール メカニズム オプションを許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。selective-acknowledgement、window-scale、および timestamp TCP オプションをクリアするには、tcp マップ コンフィギュレーション モードで **tcp-options** コマンドを使用します。明確に定義されていないオプションを持つパケットをクリアまたはドロップすることもできます。

例

次に、6 ～ 7 および 9 ～ 255 の範囲内の TCP オプションを持つすべてのパケットをドロップする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# tcp-options range 6 7 drop
hostname(config-tcp-map)# tcp-options range 9 255 drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

telnet

コンソールへの Telnet アクセスを追加し、アイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet** コマンドを使用します。以前に設定した IP アドレスから Telnet アクセスを削除するには、このコマンドの **no**
形式を使用します。

telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

no telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

構文の説明

hostname	セキュリティ アプライアンスの Telnet コンソールにアクセス可能なホストの名前を指定します。
interface_name	Telnet を実行するネットワーク インターフェイスの名前を指定します。
IP_address	セキュリティ アプライアンスへのログインが認可されているホストまたはネットワークの IP アドレスを指定します。
IPv6_address	セキュリティ アプライアンスへのログインが認可されている IPv6 アドレスおよびプレフィックスを指定します。
mask	IP アドレスに関連付けられているネットマスクを指定します。
timeout *number*	セキュリティ アプライアンスによって閉じられるまで、Telnet セッションのアイドル状態が保持される分数。有効な値は、1 ～ 1440 分です。

デフォルト

デフォルトでは、Telnet セッションは、アイドル状態のまま 5 分経過するとセキュリティ アプライアンスによって閉じられます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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)	変数 *IPv6_address* が追加されました。**no telnet timeout** コマンドも追加されました。

使用上のガイドライン

telnet コマンドを使用すると、どのホストが Telnet を使用してセキュリティ アプライアンス コンソールにアクセスできるかを指定できます。すべてのインターフェイスでセキュリティ アプライアンスへの Telnet をイネーブルにすることができます。ただし、セキュリティ アプライアンスは、すべての Telnet トラフィックを IPSec で保護された外部インターフェイスへ強制的に転送します。外部インター

フェイスへの Telnet セッションをイネーブルにするには、セキュリティ アプライアンスによって生成された IP トラフィックを外部インターフェイスの IPSec に含めるように設定し、外部インターフェイスの Telnet をイネーブルにします。

以前に設定した IP アドレスから Telnet アクセスを削除するには、**no telnet** コマンドを使用します。**telnet timeout** コマンドを使用して、コンソール Telnet セッションが、セキュリティ アプライアンスによってログオフされるまでアイドル状態を継続できる最長時間を設定できます。**no telnet** コマンドは **telnet timeout** コマンドと一緒には使用できません。

IP アドレスを入力する場合は、ネットマスクも入力する必要があります。デフォルトのネットマスクはありません。内部ネットワークのサブネットワーク マスクは使用しないでください。*netmask* は IP アドレスのビット マスクのみです。単一の IP アドレスへのアクセスを制限するには、各オクテットで 255 を使用します。たとえば、255.255.255.255 です。

IPSec が動作している場合は、セキュアでないインターフェイス名（通常、これは外部インターフェイス）を指定できます。少なくとも、**crypto map** コマンドを設定して、**telnet** コマンドで使用するインターフェイス名を指定します。

passwd コマンドを使用して、コンソールへの Telnet アクセスのパスワードを設定できます。デフォルトは **cisco** です。**who** コマンドを使用して、現在、セキュリティ アプライアンス コンソールにアクセス中の IP アドレスを表示できます。**kill** コマンドを使用すると、アクティブ Telnet コンソール セッションを終了できます。

console キーワードを指定して **aaa** コマンドを使用する場合は、Telnet コンソール アクセスを認証サーバで認証する必要があります。

（注） セキュリティ アプライアンス Telnet コンソール アクセスの認証を要求するための **aaa** コマンドが設定されているときに、コンソール ログイン要求がタイムアウトした場合は、**enable password** コマンドで設定したセキュリティ アプライアンスのユーザ名とパスワードを入力することで、シリアル コンソールからセキュリティ アプライアンスへアクセスできるようになります。

例

次に、ホスト 192.168.1.3 と 192.168.1.4 に Telnet を介したセキュリティ アプライアンス コンソールへのアクセスを許可する例を示します。さらに、192.168.2.0 ネットワーク上のすべてのホストにアクセス権が付与されています。

```
hostname(config)# telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# telnet 192.168.1.4 255.255.255.255 inside
hostname(config)# telnet 192.168.2.0 255.255.255.0 inside
hostname(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

次に、セッションの最大アイドル時間を変更する例を示します。

```
hostname(config)# telnet timeout 10
hostname(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

次に、Telnet コンソール ログイン セッションの例を示します（パスワードは、入力時に表示されません）。

```
hostname# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
hostname>
```

no telnet コマンドを使用して個々のエントリを、また、**clear configure telnet** コマンドを使用してすべての telnet コマンド ステートメントを削除できます。

```
hostname(config)# no telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

hostname(config)# clear configure telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
who	セキュリティ アプライアンス上のアクティブ Telnet 管理セッションを表示します。

terminal

現在の Telnet セッションでシステム ログ メッセージの表示を許可するには、特権 EXEC モードで **terminal monitor** コマンドを使用します。システム ログ メッセージをディセーブルにするには、**terminal no monitor** コマンドを使用します。

terminal {**monitor** | **no monitor**}

構文の説明

monitor	現在の Telnet セッションでシステム ログ メッセージの表示をイネーブルにします。
no monitor	現在の Telnet セッションでシステム ログ メッセージの表示をディセーブルにします。

デフォルト

システム ログ メッセージは、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、システム ログ メッセージを表示し、現在のセッションでシステム ログ メッセージをディセーブルにする例を示します。

```
hostname# terminal monitor
hostname# terminal no monitor
```

関連コマンド

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

terminal pager

Telnet セッションで「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定するには、特権 EXEC モードで **terminal pager** コマンドを使用します。

terminal pager [lines] *lines*

構文の説明

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

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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、現在の Telnet セッションのみを対象に、pager line 設定を変更します。新しいデフォルトの pager 設定をコンフィギュレーションに保存するには、**pager** コマンドを使用します。

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

例

次に、表示される行数を 20 に変更する例を示します。

```
hostname# terminal pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。

コマンド	説明
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージを Telnet セッションで表示できるようにします。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

terminal width

コンソール セッションで情報を表示する幅を設定するには、グローバル コンフィギュレーション モードで **terminal width** 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。

terminal width *columns*

no terminal width *columns*

構文の説明

columns	端末の幅をカラム数で指定します。デフォルト値は 80 です。指定できる範囲は 40 ～ 511 です。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、端末の表示幅を 100 カラムにする例を示します。

```
hostname# terminal width 100
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
show running-config terminal	現在の端末設定を表示します。
terminal	端末回線パラメータを特権 EXEC モードで設定します。

test aaa-server

セキュリティ アプライアンスが特定の AAA サーバでユーザを認証または認可できるかどうかを確認するには、特権 EXEC モードで **test aaa-server** コマンドを使用します。セキュリティ アプライアンス上の不正なコンフィギュレーションが原因で AAA サーバに到達できない場合があります。また、限定されたネットワーク コンフィギュレーションやサーバのダウンタイムなどの他の理由で AAA サーバに到達できないこともあります。

test aaa-server {**authentication** *server_tag* [**host** *ip_address*] [**username** *username*] [**password** *password*] | **authorization** *server_tag* [**host** *ip_address*] [**username** *username*]}

構文の説明

authentication	AAA サーバの認証機能をテストします。
authorization	AAA サーバのレガシー VPN 認可機能をテストします。
host *ip_address*	サーバの IP アドレスを指定します。コマンドで IP アドレスを指定しないと、入力を求めるプロンプトが表示されます。
password *password*	ユーザ パスワードを指定します。コマンドでパスワードを指定しないと、入力を求めるプロンプトが表示されます。
server_tag	**aaa-server** コマンドで設定した AAA サーバ タグを指定します。
username *username*	AAA サーバの設定をテストするために使用するアカウントのユーザ名を指定します。ユーザ名が AAA サーバに存在することを確認してください。存在しないと、テストは失敗します。コマンドでユーザ名を指定しないと、入力を求めるプロンプトが表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

test aaa-server コマンドでは、セキュリティ アプライアンスが特定の AAA サーバを使用してユーザを認証できることと、ユーザを認可できる場合は、レガシー VPN 認可機能を確認できます。このコマンドを使用すると、認証または認可を試みる実際のユーザを持たない AAA サーバをテストできます。また、AAA 障害の原因が、AAA サーバ パラメータの設定ミス、AAA サーバへの接続問題、またはセキュリティ アプライアンス上のその他のコンフィギュレーション エラーのいずれによるものかを特定するうえで役立ちます。

例

次に、ホスト 192.168.3.4 に srvgrp1 という RADIUS AAA サーバを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、さらに認証ポートを 1650 に設定する例を示します。AAA サーバ パラメータのセットアップの後の **test aaa-server** コマンドによって、認証テストがサーバに到達できなかったことが示されます。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: mypassword
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Rejected: Unspecified
```

次に、正常な結果となった **test aaa-server** コマンドの出力例を示します。

```
hostname# test aaa-server authentication svrgrp1 host 192.168.3.4 username bogus password
mypassword
INFO: Attempting Authentication test to IP address <10.77.152.85> (timeout: 12 seconds)
INFO: Authentication Successful
```

関連コマンド

コマンド	説明
aaa authentication console	管理トラフィックの認証を設定します。
aaa authentication match	通過するトラフィックの認証を設定します。
aaa-server	AAA サーバ グループを作成します。
aaa-server host	AAA サーバをサーバ グループに追加します。

test dynamic-access-policy attributes

dap 属性モードを入力するには、特権 EXEC モードから **test dynamic-access-policy attributes** コマンドを入力します。これにより、ユーザ属性とエンドポイント属性の値ペアを指定できます。

dynamic-access-policy attributes

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

通常、セキュリティ アプライアンスは AAA サーバからユーザ認可属性を取得し、Cisco Secure Desktop、Host Scan、CNA または NAC からエンドポイント属性を取得します。test コマンドの場合、ユーザ認可属性とエンドポイント属性をこの属性モードで指定します。セキュリティ アプライアンスは、これらの属性を、DAP サブシステムが DAP レコードの AAA 選択属性およびエンドポイント選択属性を評価するときに参照する属性データベースに書き込みます。

この機能は、DAP レコードの作成を試みます。

例

次に、**attributes** コマンドの使用例を示します。

```
hostname # test dynamic-access-policy attributes
hostname(config-dap-test-attr)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
attribute	ユーザ属性値ペアを指定できる属性モードを開始します。
display	現在の属性リストを表示します。

test dynamic-access-policy execute

test regex

正規表現をテストするには、特権 EXEC モードで **test regex** コマンドを使用します。

test regex *input_text regular_expression*

構文の説明

input_text	正規表現と一致させるテキストを指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、**regex** コマンドを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

test regex コマンドは、正規表現が一致すべきものと一致するかどうかをテストします。

正規表現が入力テキストと一致する場合は、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

正規表現が入力テキストと一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

例

次に、正規表現に対して入力テキストをテストする例を示します。

```
hostname# test regex farscape scape
INFO: Regular expression match succeeded.

hostname# test regex farscape scaper

INFO: Regular expression match failed.
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
regex	正規表現を作成します。

test sso-server

テスト用の認証要求で SSO サーバをテストするには、特権 EXEC モードで **test sso-server** コマンドを使用します。

test sso-server *server-name* **username** *user-name*

構文の説明

server-name	テストする SSO サーバの名前を指定します。
user-name	テストする SSO サーバのユーザの名前を指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。**test sso-server** コマンドは、SSO サーバが認識されるかどうか、さらに、認証要求に応答しているかどうかをテストします。

server-name 引数で指定された SSO サーバが見つからない場合は、次のエラーが表示されます。

```
ERROR: sso-server server-name does not exist
```

SSO サーバが見つかったが、*user-name* 引数で指定されたユーザが見つからない場合は、認証は拒否されます。

認証では、セキュリティ アプライアンスは SSO サーバへの WebVPN ユーザのプロキシとして動作します。セキュリティ アプライアンスは現在、SiteMinder SSO サーバ（以前の Netegrity SiteMinder）と SAML POST タイプの SSO サーバをサポートしています。このコマンドは SSO サーバの両タイプに適用されます。

例

次に、特権 EXEC モードを開始し、ユーザ名 Anyuser を使用して SSO サーバ my-sso-server をテストし、正常な結果を得た例を示します。

```
hostname# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
hostname#
```

次に、同じサーバだが、ユーザ Anotheruser でテストし、認識されず、認証が失敗した例を示します。

```
hostname# test sso-server my-sso-server username Anotheruser
INFO: Attempting authentication request to sso-server my-sso-server for user Anotheruser
INFO: STATUS: Failed
hostname#
```

関連コマンド

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

text-color

ログイン ページ、ホームページ、およびファイル アクセス ページの WebVPN タイトルバーのテキストに色を設定するには、webvpn モードで **text-color** コマンドを使用します。テキストの色をコンフィギュレーションから削除して、デフォルトにリセットするには、このコマンドの no 形式を使用します。

text-color [*black* | *white* | *auto***]**

no text-color

構文の説明

auto	secondary-color コマンドの設定に基づいて黒または白を選択します。つまり、2 番めの色が黒の場合、この値は白となります。
black	タイトルバーのテキストのデフォルト色は白です。
white	色を黒に変更できます。

デフォルト

タイトルバーのテキストのデフォルト色は白です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、タイトルバーのテキストの色を黒に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# text-color black
```

関連コマンド

コマンド	説明
secondary-text-color	WebVPN ログイン ページ、ホームページ、およびファイル アクセス ページのセカンダリ テキストの色を設定します。

tftp-server

configure net コマンドまたは **write net** コマンドで使用するデフォルトの TFTP サーバとパスおよびファイル名を指定するには、グローバル コンフィギュレーション モードで **tftp-server** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 のアドレスをサポートします。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

構文の説明

interface_name	ゲートウェイ インターフェイス名を指定します。最高のセキュリティ インターフェイス以外のインターフェイスを指定した場合は、そのインターフェイスがセキュアではないことを示す警告メッセージが表示されます。
server	TFTP サーバの IP アドレスまたは名前を設定します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
filename	パスとファイル名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	現在ではゲートウェイ インターフェイスが必要です。

使用上のガイドライン

tftp-server コマンドを使用すると、**configure net** コマンドと **write net** コマンドの入力が容易になります。**configure net** コマンドまたは **write net** コマンドを入力するときに、**tftp-server** コマンドで指定した TFTP サーバを継承するか、または独自の値を指定できます。また、**tftp-server** コマンドのパスをそのまま継承したり、**tftp-server** コマンド値の末尾にパスとファイル名を追加したり、**tftp-server** コマンド値を上書きすることもできます。

セキュリティ アプライアンスがサポートする **tftp-server** コマンドは 1 つだけです。

例

次の例では、TFTP サーバを指定し、コンフィギュレーションを /temp/config/test_config ディレクトリから読み取る方法を示します。

```
hostname(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
hostname(config)# configure net
```

関連コマンド

コマンド	説明
configure net	指定した TFTP サーバとパスからコンフィギュレーションをロードします。
show running-config tftp-server	デフォルトの TFTP サーバ アドレスとコンフィギュレーション ファイルのディレクトリを表示します。

tftp-server address

クラスタ内の TFTP サーバを指定するには、電話プロキシ コンフィギュレーション モードで **tftp-server address** コマンドを使用します。電話プロキシ コンフィギュレーションから TFTP サーバを削除するには、このコマンドの **no** 形式を使用します。

tftp-server address *ip_address* [*port*] **interface** *interface*

no tftp-server address *ip_address* [*port*] **interface** *interface*

構文の説明

ip_address	TFTP サーバのアドレスを指定します。
interface *interface*	TFTP サーバが存在するインターフェイスを指定します。これは、TFTP サーバの実アドレスにする必要があります。
port	（任意）これは、TFTP サーバが TFTP 要求をリッスンするポートです。デフォルトの TFTP ポート 69 でない場合に、設定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

電話プロキシには、少なくとも 1 つの CUCM TFTP サーバを設定する必要があります。電話プロキシに対して TFTP サーバを 5 つまで設定できます。

TFTP サーバは、信頼ネットワーク上のファイアウォールの背後に存在すると想定されます。そのため、電話プロキシは IP 電話と TFTP サーバの間の要求を代行受信します。TFTP サーバは、CUCM と同じインターフェイス上に存在している必要があります。

内部 IP アドレスを使用して TFTP サーバを作成し、TFTP サーバが存在するインターフェイスを指定します。

IP 電話で、TFTP サーバの IP アドレスを次のように設定する必要があります。

- NAT が TFTP サーバ用に設定されている場合は、TFTP サーバのグローバル IP アドレスを使用します。
- NAT が TFTP サーバ用に設定されていない場合は、TFTP サーバの内部 IP アドレスを使用します。

サービス ポリシーがグローバルに適用されている場合は、TFTP サーバが存在するインターフェイスを除くすべての入力インターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。サービス ポリシーが特定のインターフェイスに適用されている場合は、指定された電話プロキシ モジュールへのインターフェイスで、TFTP トラフィックを転送し TFTP サーバに到達させるための分類ルールが作成されます。

NAT ルールを TFTP サーバに設定する場合は、分類ルールのインストール時に TFTP サーバのグローバル アドレスが使用されるように、サービス ポリシーを適用する前に、NAT ルールを設定する必要があります。

例

次に、**tftp-server address** コマンドを使用して、電話プロキシに対応する 2 つの TFTP サーバを設定する例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
hostname(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
hostname(config-phone-proxy)# media-termination address 192.168.1.4
hostname(config-phone-proxy)# tls-proxy asa_tlsp
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# cluster-mode nonsecure
```

関連コマンド

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

threat-detection basic-threat

基本的な脅威の検出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 **threat-detection basic-threat** コマンドを使用します。基本的な脅威の検出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。

threat-detection basic-threat

no threat-detection basic-threat

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

基本脅威検出は、デフォルトでイネーブルになっています。次のデフォルトのレート制限が使用されます。

表 32-1　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**平均レート**	**バースト レート**
• DoS 攻撃の検出 • 不正なパケット形式 • 接続制限の超過 • 疑わしい ICMP パケットの検出	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 400 ドロップ / 秒。
	直前の 3600 秒間で 80 ドロップ / 秒。	直近の 320 秒間で 60 ドロップ / 秒。
スキャン攻撃の検出	直前の 600 秒間で 5 ドロップ / 秒。	直前の 10 秒間で 10 ドロップ / 秒。
	直前の 3600 秒間で 4 ドロップ / 秒。	直近の 60 秒間で 8 ドロップ / 秒。
不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）（複合）	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 200 ドロップ / 秒。
	直前の 3600 秒間で 80 ドロップ / 秒。	直近の 60 秒間で 160 ドロップ / 秒。
アクセス リストによる拒否	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 800 ドロップ / 秒。
	直前の 3600 秒間で 320 ドロップ / 秒。	直近の 60 秒間で 640 ドロップ / 秒。
• 基本ファイアウォール検査に不合格 • アプリケーション インスペクションに不合格のパケット	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 1600 ドロップ / 秒。
	直前の 3600 秒間で 320 ドロップ / 秒。	直近の 60 秒間で 1280 ドロップ / 秒。
インターフェイスの過負荷	直前の 600 秒間で 2000 ドロップ / 秒。	直前の 10 秒間で 8000 ドロップ / 秒。
	直前の 3600 秒間で 1600 ドロップ / 秒。	直近の 60 秒間で 6400 ドロップ / 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

基本的な脅威の検出をイネーブルにすると、セキュリティ アプライアンスは、次の理由によるドロップ パケットとセキュリティ イベントのレートをモニタします。

- アクセス リストによる拒否
- 不正なパケット形式（invalid-ip-header や invalid-tcp-hdr-length など）
- 接続制限の超過（システム全体のリソース制限とコンフィギュレーションで設定されている制限の両方）
- DoS 攻撃の検出（無効な SPI、ステートフル ファイアウォール検査の不合格など）
- 基本ファイアウォール検査の不合格（このオプションは、ここに列挙されているファイアウォール関連のパケット ドロップすべてを含む総合レートです。インターフェイスの過負荷、アプリケーション インスペクションで不合格のパケット、スキャン攻撃の検出など、ファイアウォールに関連しないパケット ドロップは含まれていません）
- 疑わしい ICMP パケットの検出
- アプリケーション インスペクションに不合格のパケット
- インターフェイスの過負荷
- 検出されたスキャン攻撃（このオプションでは、スキャン攻撃をモニタします。たとえば、最初の TCP パケットが SYN パケットでないことや、TCP 接続で 3 ウェイ ハンドシェイクに失敗することなどです。完全なスキャンによる脅威の検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レート情報を使用し、ホストを攻撃者として分類してそれらのホストを自動的に回避するなどして対処します）。
- 不完全セッションの検出（TCP SYN 攻撃の検出やデータなし UDP セッション攻撃の検出など）

セキュリティ アプライアンスは、脅威を検出するとすぐにシステム ログ メッセージ（733100）を送信し、ASDM に警告します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

「デフォルト」の項の表 32-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。**threat-detection rate** コマンドを使用して、各イベント タイプのデフォルト設定を上書きできます。

イベント レートが超過すると、セキュリティ アプライアンスはシステム メッセージを送信します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。バースト イベント レートは、平均レート間隔の 60 分の 1 または 10 秒のうち、どちらか大きい方の値です。受信するイベントごとに、セキュリ

ティ アプライアンスは平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、セキュリティ アプライアンスはバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection rate

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにする場合は、グローバル コンフィギュレーション モードで **threat-detection rate** コマンドを使用して、各イベント タイプのデフォルトのレート制限を変更できます。**threat-detection scanning-threat** コマンドを使用してスキャンによる脅威の検出をイネーブルにする場合は、このコマンドに **scanning-threat** キーワードを指定して、ホストを攻撃者またはターゲットと見なすタイミングを設定できます。設定しない場合は、基本的な脅威の検出とスキャンによる脅威の検出の両方で、デフォルトの **scanning-threat** 値が使用されます。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。

threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

no threat-detection rate {**acl-drop** | **bad-packet-drop** | **conn-limit-drop** | **dos-drop** | **fw-drop** | **icmp-drop** | **inspect-drop** | **interface-drop** | **scanning-threat** | **syn-attack**} **rate-interval** *rate_interval* **average-rate** *av_rate* **burst-rate** *burst_rate*

構文の説明

acl-drop	アクセス リストによる拒否のためにドロップされたパケットのレート制限を設定します。
average-rate *av_rate*	平均レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。
bad-packet-drop	パケット形式に誤りがあって（invalid-ip-header や invalid-tcp-hdr-length など）拒否されたためにドロップされたパケットのレート制限を設定します。
burst-rate *burst_rate*	バースト レート制限を 0 ～ 2147483647 ドロップ/秒の範囲で設定します。バースト レートは、*N* 秒ごとの平均レートとして計算されます。*N* はバースト レート間隔です。バースト レート間隔は、**rate-interval** *rate_interval* 値の 60 分の 1 または 10 秒のうち、どちらか大きい方の値です。
conn-limit-drop	接続制限（システム全体のリソース制限とコンフィギュレーションで設定される制限の両方）を超えたためにドロップされたパケットのレート制限を設定します。
dos-drop	DoS 攻撃（無効な SPI、ステートフル ファイアウォール チェック不合格など）を検出したためにドロップされたパケットのレート制限を設定します。
fw-drop	基本ファイアウォール チェックに不合格だったためにドロップされたパケットのレート制限を設定します。このオプションは、このコマンドのファイアウォールに関連したパケット ドロップをすべて含む複合レートです。**interface-drop**、**inspect-drop**、**scanning-threat** など、ファイアウォールに関連しないドロップ レートは含まれません。
icmp-drop	不審な ICMP パケットが検出されたためにドロップされたパケットのレート制限を設定します。
inspect-drop	パケットがアプリケーション インスペクションに失敗したためにドロップされたパケットのレート制限を設定します。
interface-drop	インターフェイスの過負荷が原因でドロップされたパケットのレート制限を設定します。
rate-interval *rate_interval*	平均レート間隔を 600 ～ 2592000 秒（30 日）の範囲で設定します。レート間隔は、ドロップ数の平均値を求める期間を決定するために使用されます。また、バーストしきい値レート間隔を決定します。

scanning-threat	スキャン攻撃が検出されたためにドロップされたパケットのレート制限を設定します。このオプションでは、たとえば最初の TCP パケットが SYN パケットでない、またはスリーウェイ ハンドシェイクで TCP 接続に失敗したなどのスキャン攻撃をモニタします。完全スキャン脅威検出（**threat-detection scanning-threat** コマンドを参照）では、このスキャン攻撃レートの情報を取得し、その情報をもとにして、たとえばホストを攻撃者として分類し自動的に遮断するなどの方法で対処します。
syn-attack	TCP SYN 攻撃やデータなし UDP セッション攻撃など、不完全なセッションが原因でドロップされたパケットのレート制限を設定します。

デフォルト

threat-detection basic-threat コマンドを使用して基本的な脅威の検出をイネーブルにした場合は、次のデフォルトのレート制限が使用されます。

表 32-2　基本脅威検出のデフォルト設定

	トリガー設定	
パケット ドロップの理由	**平均レート**	**バースト レート**
• **dos-drop** • **bad-packet-drop** • **conn-limit-drop** • **icmp-drop**	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 400 ドロップ / 秒。
	直前の 3600 秒間で 100 ドロップ / 秒。	直近の 60 秒間で 400 ドロップ / 秒。
scanning-threat	直前の 600 秒間で 5 ドロップ / 秒。	直前の 10 秒間で 10 ドロップ / 秒。
	直前の 3600 秒間で 5 ドロップ / 秒。	直前の 60 秒間で 10 ドロップ / 秒。
syn-attack	直前の 600 秒間で 100 ドロップ / 秒。	直前の 10 秒間で 200 ドロップ / 秒。
	直前の 3600 秒間で 100 ドロップ / 秒。	直近の 60 秒間で 200 ドロップ / 秒。
acl-drop	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 800 ドロップ / 秒。
	直前の 3600 秒間で 400 ドロップ / 秒。	直近の 60 秒間で 800 ドロップ / 秒。
• **fw-drop** • **inspect-drop**	直前の 600 秒間で 400 ドロップ / 秒。	直前の 10 秒間で 1600 ドロップ / 秒。
	直前の 3600 秒間で 400 ドロップ / 秒。	直近の 60 秒間で 1600 ドロップ / 秒。
interface-drop	直前の 600 秒間で 2000 ドロップ / 秒。	直前の 10 秒間で 8000 ドロップ / 秒。
	直近の 3600 秒間で 2000 ドロップ / 秒。	直近の 60 秒間で 8000 ドロップ / 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

イベント タイプごとに、異なるレート間隔を 3 つまで設定できます。

基本的な脅威の検出をイネーブルにした場合、セキュリティ アプライアンスは、「構文の説明」の表で説明したイベント タイプによるドロップ パケットとセキュリティ イベントのレートをモニタします。

セキュリティ アプライアンスは、脅威を検出するとすぐにシステム ログ メッセージ（733100）を送信し、ASDM に警告します。

基本脅威検出は、ドロップや潜在的な脅威があった場合に限りパフォーマンスに影響を与えます。この状況でも、パフォーマンスへの影響は大きくありません。

「デフォルト」の項の表 32-1 に、デフォルト設定を示します。すべてのデフォルト設定は、**show running-config all threat-detection** コマンドを使用して表示できます。

イベント レートが超過すると、セキュリティ アプライアンスはシステム メッセージを送信します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。受信するイベントごとに、セキュリティ アプライアンスは平均レート制限とバースト レート制限をチェックします。両方のレートが超過している場合、セキュリティ アプライアンスはバースト期間あたりのレート タイプごとに最大 1 つのメッセージを生成して、2 つの異なるシステム メッセージを送信します。

例

次の例では、基本脅威検出をイネーブルにし、DoS 攻撃のトリガーを変更しています。

```
hostname(config)# threat-detection basic-threat
hostname(config)# threat-detection rate dos-drop rate-interval 600 average-rate 60
burst-rate 100
```

関連コマンド

コマンド	説明
clear threat-detection rate	基本脅威検出の統計情報をクリアします。
show running-config all threat-detection	脅威検出コンフィギュレーションを表示します。個別にレート設定をしていない場合はデフォルトのレート設定も表示されます。
show threat-detection rate	基本脅威検出の統計情報を表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。

threat-detection scanning-threat

スキャンによる脅威の検出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 **threat-detection scanning-threat** コマンドを使用します。スキャンによる脅威の検出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。

threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

no threat-detection scanning-threat [**shun**
[**except** {**ip-address** *ip_address mask* | **object-group** *network_object_group_id*} |
duration *seconds*]]

構文の説明

duration *seconds*	攻撃元ホストの回避期間を 10 ～ 2592000 秒の範囲で設定します。デフォルトの期間は 3600 秒（1 時間）です。
except	IP アドレスを回避対象から除外します。このコマンドを複数回入力し、複数の IP アドレスまたはネットワーク オブジェクト グループを特定して遮断対象から除外できます。
ip-address *ip_address mask*	回避対象から除外する IP アドレスを指定します。
object-group *network_object_group_id*	回避対象から除外するネットワーク オブジェクト グループを指定します。オブジェクト グループを作成するには、**object-group network** コマンドを参照してください。
shun	セキュリティ アプライアンスがホストを攻撃者と識別するとホスト接続を自動的に終了し、さらに、システム ログ メッセージ 733101 を送信します。

デフォルト

デフォルトの回避期間は 3600 秒（1 時間）です。

スキャン攻撃イベントでは、次のデフォルトのレート制限が使用されます。

表 32-3　スキャンによる脅威の検出のデフォルトのレート制限

平均レート	バースト レート
直前の 600 秒間で 5 ドロップ / 秒。	直前の 10 秒間で 10 ドロップ / 秒。
直前の 3600 秒間で 5 ドロップ / 秒。	直前の 60 秒間で 10 ドロップ / 秒。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**duration** キーワードが追加されました。

使用上のガイドライン

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、セキュリティ アプライアンス のスキャンによる脅威の検出機能では、広範なデータベースが保持され、これに含まれるホスト統計情報をスキャン アクティビティに関する分析に使用できます。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

注意　スキャンによる脅威の検出機能は、ホストおよびサブネットベースのデータ構造を作成し情報を収集する間、セキュリティ アプライアンスのパフォーマンスとメモリに大きく影響することがあります。

攻撃者に関するシステム ログ メッセージを送信するように セキュリティ アプライアンス を設定したり、自動的にホストを排除したりできます。デフォルトでは、ホストが攻撃者であると識別されると、システム ログ メッセージ 733101 が生成されます。

セキュリティ アプライアンスは、スキャンによる脅威イベント レートを超過した時点で、攻撃者とターゲットを識別します。セキュリティ アプライアンスは、一定間隔における平均イベント レートと短期バースト間隔におけるバースト イベント レートの 2 種類のレートを追跡します。スキャン攻撃の一部と見なされるイベントが検出されるたびに、セキュリティ アプライアンスは平均レート制限とバースト レート制限をチェックします。ホストから送信されるトラフィックがどちらかのレートを超えると、そのホストは攻撃者と見なされます。ホストが受信したトラフィックがどちらかのレートを超えると、そのホストはターゲットと見なされます。スキャンによる脅威イベントのレート制限は **threat-detection rate scanning-threat** コマンドを使用して変更できます。

攻撃者またはターゲットとして分類されたホストを表示するには、**show threat-detection scanning-threat** コマンドを使用します。

回避対象のホストを表示するには、**show threat-detection shun** コマンドを使用します。排除対象からホストを除外するには、**clear threat-detection shun** コマンドを使用します。

例

次に、スキャンによる脅威の検出をイネーブルにし、10.1.1.0 ネットワーク上のホストを除き、攻撃者として分類されたホストを自動的に回避する例を示します。スキャンによる脅威の検出のデフォルトのレート制限は変更することもできます。

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection rate scanning-threat rate-interval 1200 average-rate 10
burst-rate 20
hostname(config)# threat-detection rate scanning-threat rate-interval 2400 average-rate 10
burst-rate 20
```

関連コマンド

コマンド	説明
clear threat-detection shun	ホストを回避対象から解除します。
show threat-detection scanning-threat	攻撃者およびターゲットとして分類されたホストを表示します。
show threat-detection shun	現在回避されているホストを表示します。
threat-detection basic-threat	基本脅威検出をイネーブルにします。
threat-detection rate	イベント タイプごとの脅威検出レート制限を設定します。

threat-detection statistics

スキャンによる脅威の検出の統計情報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 **threat-detection statistics** コマンドを使用します。スキャンによる脅威の検出の統計情報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。

注意　統計情報をイネーブルにすると、イネーブルにした統計情報のタイプに応じて、セキュリティ アプライアンスのパフォーマンスに影響することがあります。**threat-detection statistics host** コマンドはパフォーマンスに大幅に影響を与えるため、トラフィックの負荷が高い場合は、このタイプの統計情報を一時的にイネーブルにすることを検討します。ただし、**threat-detection statistics port** コマンドは大きな影響を与えません。

threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

no threat-detection statistics [**access-list** | **host** | **port** | **protocol** | **tcp-intercept** [**rate-interval** *minutes*] [**burst-rate** *attacks_per_sec*] [**average-rate** *attacks_per_sec*]]

構文の説明

access-list	（任意）アクセス リストによる拒否の統計情報をイネーブルにします。アクセス リスト統計情報は、**show threat-detection top access-list** コマンドを使用した場合にだけ表示されます。
average-rate *attacks_per_sec*	（任意）TCP 代行受信について、syslog メッセージ生成の平均レートしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 200 回です。平均レートがこれを超えると、syslog メッセージ 733105 が生成されます。
burst-rate *attacks_per_sec*	（任意）TCP 代行受信について、syslog メッセージ生成のしきい値を 25 ～ 2147483647 の範囲で指定します。デフォルトは 1 秒間に 400 です。バースト レートがこれを超えると、syslog メッセージ 733104 が生成されます。
host	（任意）ホスト統計情報をイネーブルにします。ホスト統計情報は、ホストがアクティブであり、スキャン脅威ホスト データベース内にある間は蓄積されます。ホストは、非アクティブになってから 10 分後にデータベースから削除されます（統計情報もクリアされます）。
port	（任意）ポート統計情報をイネーブルにします。
protocol	（任意）プロトコル統計情報をイネーブルにします。
rate-interval *minutes*	（任意）TCP 代行受信について、履歴モニタリング ウィンドウのサイズを、1 ～ 1440 分の範囲で設定します。デフォルトは 30 分です。この間に、セキュリティ アプライアンスが攻撃をサンプリングする回数は 60 回です。
tcp-intercept	（任意）TCP 代行受信によって代行受信される攻撃の統計情報をイネーブルにします。TCP 代行受信をイネーブルにするには、**set connection embryonic-conn-max コマンド**、**nat** コマンド、または **static** コマンドを参照してください。

デフォルト

デフォルトでは、アクセス リスト統計情報はイネーブルです。このコマンドにオプションを指定しなかった場合は、すべてのオプションがイネーブルになります。

デフォルトの **tcp-intercept rate-interval** は 30 分です。デフォルトの **burst-rate** は 1 秒あたり 400 です。デフォルトの **average-rate** は 1 秒あたり 200 です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。
8.0(4)	**tcp-intercept** キーワードが追加されました。

使用上のガイドライン　統計情報を表示するには、**show threat-detection statistics** コマンドを使用します。

threat-detection scanning-threat コマンドを使用して、スキャンによる脅威の検出をイネーブルにする必要はありません。検出と統計情報は個別に設定できます。

例　次に、ホストを除くすべてのタイプのスキャンによる脅威の検出とスキャン脅威統計情報の例を示します。

```
hostname(config)# threat-detection scanning-threat shun except ip-address 10.1.1.0
255.255.255.0
hostname(config)# threat-detection statistics access-list
hostname(config)# threat-detection statistics port
hostname(config)# threat-detection statistics protocol
hostname(config)# threat-detection statistics tcp-intercept
```

関連コマンド

コマンド	説明
threat-detection scanning-threat	脅威検出のスキャンをイネーブルにします。
show threat-detection statistics host	ホストの統計情報を表示します。
show threat-detection statistics port	ポートの統計情報を表示します。
show threat-detection statistics protocol	プロトコルの統計情報を表示します。
show threat-detection statistics top	上位 10 位までの統計情報を表示します。

threshold

SLA モニタリング動作のしきい値超過イベントのしきい値を設定するには、SLA モニタ コンフィギュレーション モードで **threshold** 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。

threshold *milliseconds*

no threshold

構文の説明

milliseconds	宣言する上昇しきい値をミリ秒で指定します。有効な値は、0 ～ 2147483647 です。この値は、タイムアウトに設定された値以下にする必要があります。

デフォルト

デフォルトのしきい値は 5000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

しきい値は、しきい値超過イベントを示すためにだけ使用されます。到達可能性には影響しませんが、**timeout** コマンドの適切な設定を評価するために使用できます。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

timeout

さまざまな機能に対応するグローバルな最大アイドル時間を設定するには、グローバル コンフィギュレーション モードで **timeout** コマンドを使用します。すべてのタイムアウトをデフォルトに戻すには、このコマンドの **no** 形式を使用します。単一の機能をデフォルトにリセットするには、**timeout** コマンドにデフォルト値を指定して再度入力します。

timeout {**xlate** | **conn** | **udp** | **icmp** | **rpc** | **h225** | **h323** | **mgcp** | **mgcp-pat** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media** | **sip-provisional-media** | **tcp-proxy-reassembly**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

no timeout

構文の説明

absolute	（任意）uauth timeout が期限切れになった後、再認証を要求します。デフォルトでは、**absolute** キーワードはイネーブルです。非アクティブな状態が一定時間経過した後 uauth タイマーがタイムアウトするように設定するには、代わりに **inactivity** キーワードを入力します。
conn	（任意）接続を閉じた後のアイドル時間を 0:05:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
hh:*mm*:*ss*	タイムアウトを、時間、分、秒で指定します。接続をタイムアウトしない場合は、**0** を使用します（可能な場合）。
h225	（任意）H.225 シグナリング接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 1 時間（1:0:0）です。タイムアウト値を 0:0:01 に指定すると、タイマーはディセーブルになり、TCP 接続はすべてのコールがクリアされるとすぐに切断されます。
h323	（任意）H.245（TCP）および H.323（UDP）メディア接続を閉じるまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。H.245 と H.323 のいずれのメディア接続にも同じ接続フラグが設定されているため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
half-closed	（任意）TCP half-closed 接続を解放するまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
icmp	（任意）ICMP のアイドル時間を 0:0:02 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 秒（0:0:02）です。
inactivity	（任意）非アクティブ タイムアウトが期限切れになった後、uauth 再認証を要求します。
mgcp	（任意）MGCP メディア接続を削除するまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは、5 分（0:5:0）です。
mgcp-pat	（任意）MGCP PAT 変換を削除するまでの絶対間隔を 0:0:0 ～ 1193:0:0 の範囲で設定します。デフォルトは 5 分（0:5:0）です。
rpc	（任意）RPC スロットを解放するまでのアイドル時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、5 分（0:05:0）です。
sip	（任意）SIP 制御接続を閉じるまでのアイドル時間を 0:5:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、30 分（0:30:0）です。接続がタイムアウトしないようにするには、**0** を使用します。

sip-disconnect	（任意）CANCEL メッセージまたは BYE メッセージで 200 OK を受信しなかった場合に、SIP セッションを削除するまでのアイドル時間を 0:0:1 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。
sip-invite	（任意）暫定応答のピンホールとメディア xlate を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは、3 分（0:3:0）です。
sip_media	（任意）SIP メディア接続を閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。 SIP メディア タイマーは、SIP UDP メディア パケットを使用する SIP RTP/RTCP で、UDP 非アクティブ タイムアウトの代わりに使用されます。
sip-provisional-media	（任意）SIP プロビジョナル メディア接続のタイムアウト値を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 2 分（0:2:0）です。
sunrpc	（任意）SUNRPC スロットを閉じるまでのアイドル時間を 0:1:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 10 分（0:10:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
tcp-proxy-reassembly	（任意）再構築のためバッファ内で待機しているパケットをドロップするまでのアイドル タイムアウトを 0:0:10 ～ 1193:0:0 の範囲で設定します。デフォルトは、1 分（0:1:0）です。
uauth	（任意）認証および認可キャッシュがタイムアウトし、ユーザが次回接続時に再認証が必要となるまでの継続時間を 0:0:0 ～ 1193:0:0 の範囲で指定します。デフォルトは 5 分（0:5:0）です。デフォルトのタイマーは absolute です。**inactivity** キーワードを入力すると、無活動の期間後にタイムアウトが発生するように設定できます。**uauth** 継続時間は、**xlate** 継続時間より短く設定する必要があります。キャッシュをディセーブルにするには、**0** に設定します。接続に受動 FTP を使用している場合、または Web 認証に **virtual http** コマンドを使用している場合は、**0** を使用しないでください。
udp	（任意）UDP スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 2 分（0:2:0）です。接続がタイムアウトしないようにするには、**0** を使用します。
xlate	（任意）変換スロットが解放されるまでのアイドル時間を指定します。有効な値は 0:1:0 ～ 1193:0:0 です。デフォルトは 3 時間（3:0:0）です。

デフォルト

デフォルトの設定は次のとおりです。

- **conn** *hh*:*mm*:*ss* は 1 時間（**1:0:0**）です。
- **h225** *hh*:*mm*:*ss* は 1 時間（**1:0:0**）です。
- **h323** *hh*:*mm*:*ss* は 5 分（**0:5:0**）です。
- **half-closed** *hh*:*mm*:*ss* は 10 分（**0:10:0**）です。
- **icmp** *hh:mm:ss* は 2 秒（**0:0:2**）です。
- **mgcp** *hh:mm:ss* は 5 分（**0:5:0**）です。
- **mgcp-pat** *hh:mm:ss* は 5 分（**0:5:0**）です。
- **rpc** *hh*:*mm*:*ss* は 5 分（**0:5:0**）です。
- **sip** *hh:mm:* は 30 分（**0:30:0**）です。
- **sip-disconnect** *hh:mm:ss* は 2 分（**0:2:0**）です。
- **sip-invite** *hh:mm:ss* は 3 分（**0:3:0**）です。

- **sip_media** *hh:mm:ss* は 2 分（**0:2:0**）です。
- **sip-provisional-media** *hh:mm:ss* は 2 分（**0:2:0**）です。
- **sunrpc** *hh:mm:ss* は、10 分（**0:10:0**）です。
- **tcp-proxy-reassembly** *hh:mm:ss* は 1 分（**0:1:0**）です。
- **uauth** *hh:mm:ss* は 5 分（**00:5:00**）**絶対時間**です。
- **udp** *hh*:*mm*:*ss* は 2 分（**00:02:00**）です。
- **xlate** *hh*:*mm*:*ss* は 3 時間（**03:00:00**）です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	**mgcp-pat**、**sip-disconnect**、および **sip-invite** キーワードが追加されました。
7.2(4)/8.0(4)	**sip-provisional-media** キーワードが追加されました。
7.2(5)/8.0(5)	**tcp-proxy-reassembly** キーワードが追加されました。

使用上のガイドライン　**timeout** コマンドを使用すると、グローバルにタイムアウトを設定できます。一部の機能では、コマンドで指定されたトラフィックに対し、**set connection timeout** コマンドが優先されます。

timeout コマンドの後に、キーワードと値を複数入力できます。

接続タイマー（**conn**）は変換タイマー（**xlate**）より優先されます。変換タイマーは、すべての接続がタイムアウトになった後にのみ動作します。

例　次に、最大アイドル時間を設定する例を示します。

```
hostname(config)# timeout uauth 0:5:0 absolute uauth 0:4:0 inactivity
hostname(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

関連コマンド

コマンド	説明
clear configure timeout	タイムアウト コンフィギュレーションをクリアし、デフォルトにリセットします。
set connection timeout	Modular Policy Framework を使用して接続タイムアウトを設定します。
show running-config timeout	指定されたプロトコルのタイムアウト値を表示します。

timeout（AAA サーバ ホスト）

AAA サーバとの接続確立を中断するまでに許容される、ホスト固有の最大応答時間を秒単位で設定するには、aaa サーバ ホスト モードで **timeout** コマンドを使用します。タイムアウト値を削除し、タイムアウトをデフォルト値の 10 秒にリセットするには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout

構文の説明

seconds	要求のタイムアウト間隔（1 ～ 60 秒）を指定します。この時間を超えると、セキュリティ アプライアンスはプライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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
7.0(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

このコマンドはすべての AAA サーバ プロトコル タイプで有効です。

セキュリティ アプライアンスが AAA サーバへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。**retry-interval** コマンドを使用して、セキュリティ アプライアンスが各接続試行の間で待機する時間を指定できます。

タイムアウトは、セキュリティ アプライアンスがサーバとのトランザクションの完了を試みて費やす時間の合計です。再試行間隔は、タイムアウト期間中に通信を再試行する頻度を決定します。そのため、再試行間隔をタイムアウト値以上にすると、再試行は行われません。再試行が実行されるようにするには、再試行間隔をタイムアウト値より小さくする必要があります。

例

次に、ホスト 1.2.3.4 の RADIUS AAA サーバ「svrgrp1」が 30 秒のタイムアウト値と 10 秒の再試行間隔を使用するように設定する例を示します。セキュリティ アプライアンスは、30 秒後に通信試行を中断するまでに 3 回試行を繰り返します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
```

```
hostname(config-aaa-server-host)# timeout 30
hostname(config-aaa-server-host)# retry-interval 10
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa	現在の AAA コンフィギュレーションの値を表示します。

timeout（dns サーバ グループ コンフィギュレーション モード）

次の DNS サーバを試行するまでの待機時間の合計を指定するには、dns サーバ グループ コンフィギュレーション モードで **timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout [*seconds*]

構文の説明

seconds	タイムアウトを 1 ～ 30 の範囲で指定します（秒単位）。デフォルトは 2 秒です。セキュリティ アプライアンスがサーバのリストを再試行するたびに、このタイムアウトは倍増します。dns サーバ グループ コンフィギュレーション モードで **retries** コマンドを使用して、再試行回数を設定できます。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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
7.1(1)	このコマンドが導入されました。

例

次に、DNS サーバ グループ「dnsgroup1」のタイムアウトを 1 秒に設定する例を示します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns timeout 1
```

関連コマンド

コマンド	説明
clear configure dns	ユーザが作成した DNS サーバ グループをすべて削除し、デフォルト サーバ グループの属性をデフォルト値にリセットします。
domain-name	デフォルトのドメイン名を設定します。

コマンド	説明
retries	セキュリティ アプライアンスが応答を受信しないときに、DNS サーバのリストを再試行する回数を指定します。
show running-config dns server-group	現在の実行中の DNS サーバ グループ コンフィギュレーションを表示します。

timeout（gtp マップ）

GTP セッションの非アクティブ タイマーを変更するには、**gtp-map** コマンドを使用してアクセスする GTP マップ コンフィギュレーション モードで **timeout** コマンドを使用します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

no timeout {**gsn** | **pdp-context** | **request** | **signaling** | **t3-response** | **tunnel** } *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン（:）で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。
gsn	GSN を削除するまでの非アクティブな期間を指定します。
pdp-context	PDP コンテキストの受信を開始する前に許容される最大時間を指定します。
request	GTP メッセージの受信を開始する前に許容される最大時間を指定します。
signaling	GTP シグナリングを削除するまでの非アクティブな期間を指定します。
t3-response	GTP 接続を削除する前に応答を待機する最大時間を指定します。
tunnel	GTP トンネルを切断するまでの非アクティブな期間を指定します。

デフォルト

gsn、**pdp-context**、および **signaling** のデフォルトは 30 分です。

request のデフォルトは 1 分です。

tunnel のデフォルトは 1 時間です（PDP コンテキスト削除要求を受信しない場合）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル（PDP）コンテキストは、IMSI と NSAPI との組み合わせである Tunnel Identifier（TID; トンネル ID）によって識別されます。各 MS は最大 15 の NSAPI を保持できるため、多様な QoS レベルのアプリケーション要件に基づいて、それぞれ異なる NSAPI を持つ PDP コンテキストを複数作成できます。

GTP トンネルは、異なる GSN ノードにある 2 個の関連する PDP コンテキストによって定義され、1 つのトンネル ID によって識別されます。GTP トンネルは、外部パケット データ ネットワークとモバイル ステーション ユーザの間でパケットを転送するために必要です。

例

次に、要求キューのタイムアウト値を 2 分に設定する例を示します。

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# timeout request 00:02:00
```

関連コマンド

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

timeout（RADIUS アカウンティング）

RADIUS アカウンティング ユーザの非アクティブ タイマーを変更するには、**inspect radius-accounting** コマンドを使用してアクセスする radius アカウンティング パラメータ コンフィギュレーション モードで **timeout** コマンドを使用します。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

構文の説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン（:）で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。デフォルトは 1 時間です。
users	ユーザのタイムアウトを指定します。

デフォルト

ユーザのデフォルトのタイムアウトは 1 時間です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

次に、ユーザのタイムアウト値を 10 分に設定する例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout user 00:10:00
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

timeout（sla モニタ）

SLA 動作が要求パケットへの応答を待機する時間を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで、**timeout** 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。

timeout *milliseconds*

no timeout

構文の説明

milliseconds	0 ～ 604800000

デフォルト

デフォルトのタイムアウト値は 5000 ミリ秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

frequency コマンドを使用して、SLA 動作が要求パケットを送信する頻度を設定し、**timeout** コマンドを使用して、SLA 動作がそれらの要求への応答の受信を待機する時間を設定できます。**timeout** コマンドには、**frequency** コマンドに指定する値より大きい値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA 動作を繰り返す頻度を指定します。
sla monitor	SLA モニタリング動作を定義します。

timeout pinhole

DCERPC ピンホールのタイムアウトを設定し、2 分のグローバル システム ピンホール タイムアウトを上書きするには、パラメータ コンフィギュレーション モードで **timeout pinhole** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。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。

timeout pinhole *hh:mm:ss*

no timeout pinhole

構文の説明

hh:mm:ss	ピンホール接続のタイムアウト。指定できる値は 0:0:1 ～ 1193:0:0 です。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

次に、DCERPC インスペクション ポリシー マップでピンホール接続のピンホール タイムアウトを設定する例を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout pinhole 0:10:00
```

関連コマンド

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

time-range

時間範囲コンフィギュレーション モードを開始し、トラフィック ルールにアタッチできる時間範囲、またはアクションを定義するには、グローバル コンフィギュレーション モードで **time-range** 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。

time-range *name*

no time-range *name*

構文の説明

name　時間範囲の名前。名前は 64 文字以下にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間範囲を作成してもデバイスへのアクセスは制限されません。**time-range** コマンドは時間範囲のみを定義します。時間範囲を定義した後、それをトラフィック ルールまたはアクションにアタッチできます。

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

時間範囲はセキュリティ アプライアンスのシステム クロックに依存しています。ただし、この機能は、NTP 同期化により最適に動作します。

例

次に、時間範囲「New_York_Minute」を作成し、時間範囲コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# time-range New_York_Minute
hostname(config-time-range)#
```

時間範囲を作成し、時間範囲コンフィギュレーション モードを開始した後、**absolute** コマンドと **periodic** コマンドを使用して時間範囲パラメータを定義できます。**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻すには、時間範囲コンフィギュレーション モードで **default** コマンドを使用します。

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** コマンドを使用して、時間範囲を ACL にバインドします。次に、ACL「Sales」を時間範囲「New_York_Minute」にバインドする例を示します。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

ACL の詳細については、**access-list extended** コマンドを参照してください。

関連コマンド

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

timeout secure-phones

電話プロキシ データベースからセキュア フォン エントリを削除するまでのアイドル タイムアウトを設定するには、電話プロキシ コンフィギュレーション モードで **timeout secure-phones** コマンドを使用します。タイムアウト値をデフォルトの 5 分に戻すには、このコマンドの **no** 形式を使用します。

timeout secure-phones *hh:mm:ss*

no timeout secure-phones *hh:mm:ss*

構文の説明

hh:mm:ss	オブジェクトを削除するまでのアイドル タイムアウトを指定します。デフォルトは 5 分です。

デフォルト

セキュア フォン タイムアウトのデフォルト値は 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

セキュア フォンによって起動時に必ず CTL ファイルが要求されるため、電話プロキシは、電話をセキュアとしてマークするデータベースを作成します。セキュア フォン データベースのエントリは、設定された指定タイムアウト後に（**timeout secure-phones** コマンドを介して）削除されます。エントリのタイムスタンプは、電話プロキシが SIP 電話の登録更新および SCCP 電話のキープアライブを受信するたびに更新されます。

timeout secure-phones コマンドのデフォルト値は 5 分です。SCCP キープアライブおよび SIP レジスタ更新の最大タイムアウト値より大きい値を指定します。たとえば、SCCP キープアライブが 1 分間隔に指定され、SIP レジスタ更新が 3 分に設定されている場合は、このタイムアウト値には 3 分より大きい値を設定します。

例

次に、**timeout secure-phones** コマンドを使用して、電話プロキシが 3 分後にセキュア フォン データベースのエントリをタイムアウトにするように設定する例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)# tftp-server address 192.168.1.2 in interface outside
hostname(config-phone-proxy)# tftp-server address 192.168.1.3 in interface outside
hostname(config-phone-proxy)# media-termination address 192.168.1.4
hostname(config-phone-proxy)# tls-proxy asa_tlsp
```

```
hostname(config-phone-proxy)# ctl-file asactl
hostname(config-phone-proxy)# timeout secure-phones 00:03:00
```

関連コマンド

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

timers lsa-group-pacing

OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を指定するには、ルータ コンフィギュレーション モードで **timers lsa-group-pacing** 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。

timers lsa-group-pacing *seconds*

no timers lsa-group-pacing [*seconds*]

構文の説明

seconds	OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔。有効な値は、10 ～ 1800 秒です。

デフォルト

デフォルトの間隔は 240 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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
既存	このコマンドは既存です。

使用上のガイドライン

OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を 1 つのグループに収集し、更新、チェックサム、または期限切れにする間隔を変更するには **timers lsa-group-pacing** *seconds* コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers lsa-group-pacing** コマンドを使用します。

例

次に、LSA のグループ処理間隔を 500 秒に設定する例を示します。

```
hostname(config-router)# timers lsa-group-pacing 500
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。

コマンド	説明
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
timers spf	Shortest Path First（SPF; 最短パス優先）計算遅延とホールド タイムを指定します。

timers spf

Shortest Path First（SPF; 最短パス優先）計算遅延とホールド タイムを指定するには、ルータ コンフィギュレーション モードで **timers spf** 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。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

構文の説明

delay	OSPF がトポロジ変更を受信してから Shortest Path First（SPF; 最短パス優先）計算を開始するまでの遅延時間を 1 ～ 65535 の範囲（秒単位）で指定します。
holdtime	2 つの連続する SPF 計算の間のホールド タイム（秒単位）。有効な値は、1 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

- *delay* は 5 秒です。
- *holdtime* は 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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
既存	このコマンドは既存です。

使用上のガイドライン

OSPF プロトコルがトポロジ変更を受信してから計算を開始するまでの遅延時間と、2 つの連続する SPF 計算の間のホールド タイムを設定するには、**timers spf** コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers spf** コマンドを使用します。

例

次に、SPF 計算遅延を 10 秒に設定し、SPF 計算ホールド タイムを 20 秒に設定する例を示します。

```
hostname(config-router)# timers spf 10 20
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。

コマンド	説明
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
timers lsa-group-pacing	OSPF Link-State Advertisements（LSA; リンク ステート アドバタイズメント）を収集し、更新、チェックサム、または期限切れにする間隔を指定します。

title

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する WebVPN ページのタイトル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 **title** コマンドを使用します。

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

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

構文の説明

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

デフォルト

デフォルトのタイトルのテキストは「WebVPN Service」です。

デフォルトのタイトル スタイルは、次のとおりです。

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger;
vertical-align:middle;text-align:left;font-weight:bold

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

タイトルを付けない場合は、*value* 引数を指定せずに **title text** コマンドを使用します。

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

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

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

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

例

次の例では、タイトルがテキスト「Cisco WebVPN Service」でカスタマイズされています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

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。
page style	Cascading Style Sheet（CSS; カスケーディング スタイル シート）パラメータを使用して WebVPN ページをカスタマイズします。

tls-proxy

TLS コンフィギュレーション モードで TLS プロキシ インスタンスを設定したり、最大セッション数を設定したりするには、グローバル コンフィギュレーション モードで **tls-proxy** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

no tls-proxy [**maximum-sessions** *max_sessions* | *proxy_name*] [**noconfirm**]

構文の説明

max_sessions *max_sessions*	プラットフォームでサポートする TLS プロキシ セッションの最大数を指定します。
noconfirm	確認を要求せずに **tls-proxy** コマンドを実行します。
proxy_name	TLS プロキシ インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

tls-proxy コマンドを使用して TLS プロキシ コンフィギュレーション モードを開始し、TLS プロキシ インスタンスを作成したり、プラットフォームでサポートされる最大セッション数を設定したりできます。

例

次の例では、TLS プロキシ インスタンスを作成する方法を示します。

```
hostname(config)# tls-proxy my_proxy
hostname(config-tlsp)# server trust-point ccm_proxy
hostname(config-tlsp)# client ldc issuer ldc_server
hostname(config-tlsp)# client ldc keypair phone_common
```

関連コマンド

コマンド	説明
client	暗号スイートを定義し、ローカル ダイナミック証明書の発行者またはキーペアを設定します。
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。

tos

SLA 動作要求パケットの IP ヘッダー内のタイプ オブ サービス バイトを定義するには、SLA モニタ プロトコル コンフィギュレーション モードで **tos** 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。

tos *number*

no tos

構文の説明

number	IP ヘッダーで使用するサービス タイプの値。有効な値は、0 ～ 255 です。

デフォルト

デフォルトのタイプ オブ サービス値は 0 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。これは、専用アクセス レートなどのポリシー ルーティングおよび機能のために、ネットワーク上の他のルータによって使用されます。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。エコー要求パケットのペイロード サイズを 48 バイトに設定し、SLA 動作中に送信されるエコー要求数を 5 に、さらにタイプ オブ サービス バイトを 80 に設定します。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# tos 80
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA 動作をエコー応答時間プローブ動作として設定します。

traceroute

パケットが宛先に到達するまでにたどるルートを調査するには、**traceroute** コマンドを使用します。

traceroute *destination_ip* | *hostname* [**source** *source_ip* | *source-interface*] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

構文の説明

destination_ip	traceroute の宛先 IP アドレスを指定します。
hostname	ルートをトレースする先のホストのホスト名。ホスト名を指定する場合は、**name** コマンドで定義するか、traceroute をイネーブルにしてホスト名を IP アドレスに解決するように DNS サーバを設定します。www.example.com などの DNS ドメイン名をサポートします。
source	トレース パケットの送信元として使用される IP アドレスまたはインターフェイスを指定します。
source_ip	パケット トレースの送信元 IP アドレスを指定します。この IP アドレスはいずれかのインターフェイスの IP アドレスにする必要があります。トランスペアレント モードでは、セキュリティ アプライアンスの管理 IP アドレスにする必要があります。
source_interface	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。指定する場合は、送信元インターフェイスの IP アドレスが使用されます。
numeric	出力に中間ゲートウェイの IP アドレスのみが示されるように指定します。このキーワードを指定しない場合は、トレース中に到達したゲートウェイのホスト名の検索を試みます。
timeout	使用されるタイムアウト値を指定します。
timeout_value	接続をタイムアウトにする前に応答を待機する時間を指定します。デフォルトは 3 秒です。
probe *probe_num*	TTL の各レベルで送信するプローブの数。デフォルト数は 3 です。
ttl	プローブで使用する存続可能時間の値の範囲を指定するキーワード。
min_ttl	最初のプローブの TTL 値。デフォルトは 1 ですが、既知のホップの表示を抑制するためにより大きい値を設定できます。
max-ttl	使用可能な最大 TTL 値。デフォルト値は 30 です。traceroute パケットが宛先に到達するか、値に達したときにコマンドは終了します。
port *port_value*	ユーザ データグラム プロトコル（UDP）プローブ メッセージによって使用される宛先ポート。デフォルト値は 33434 です。
use-icmp	UDP プローブ パケットの代わりに ICMP プローブ パケットを使用するように指定します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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
特権 EXEC	•	•	•	•	•

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

traceroute コマンドは送信した各プローブの結果を示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次に、**traceroute** コマンドによって表示される出力記号を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP プロトコルに到達できません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

例

次に、宛先 IP アドレスを指定した場合の traceroute 出力の例を示します。

```
hostname# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
packet-tracer	パケット トレース機能をイネーブルにします。

track rtr

SLA 動作の到達可能性を追跡するには、グローバル コンフィギュレーション モードで **track rtr** コマンドを使用します。SLA 追跡を削除するには、このコマンドの **no** 形式を使用します。

track *track-id* **rtr** *sla-id* **reachabilitity**

no track *track-id* **rtr** *sla-id* **reachabilitity**

構文の説明

reachability	オブジェクトの到達可能性を追跡するように指定します。
sla-id	トラッキング エントリが使用する SLA の ID。
track-id	トラッキング エントリ オブジェクト ID を作成します。有効な値は、1 ～ 500 です。

デフォルト

SLA 追跡はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

track rtr コマンドは、トラッキング エントリ オブジェクト ID を作成し、トラッキング エントリが使用する SLA を指定します。

各 SLA 動作が、トラッキング プロセスによって解釈される動作戻りコード値を維持します。戻りコードには、OK や Over Threshold などのいくつかの戻りコードがあります。表 32-4 は、これらの戻りコードに関連するオブジェクトの到達可能性ステートを表示します。

表 32-4　SLA 追跡の戻りコード

トラッキング	戻りコード	追跡ステート
Reachability	OK または Over Threshold	Up
	他の任意のコード	Down

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
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
```

関連コマンド

コマンド	説明
route	スタティック ルートを設定します。
sla monitor	SLA モニタリング動作を定義します。

traffic-non-sip

既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可するには、パラメータ コンフィギュレーション モードで **traffic-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。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。

traffic-non-sip

no traffic-non-sip

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、SIP インスペクション ポリシー マップで既知の SIP シグナリング ポートを使用する非 SIP トラフィックを許可する例を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# traffic-non-sip
```

関連コマンド

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

transfer-encoding

転送エンコーディング タイプを指定して HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセス可能な HTTP マップ コンフィギュレーション モードで、**transfer-encoding** 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。

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**allow** | **reset** | **drop**} [**log**]

構文の説明

action	指定した転送エンコーディング タイプを使用する接続が検出されたときに実行するアクションを指定します。
allow	メッセージを許可します。
chunked	メッセージ本文を一連のチャンクとして転送する転送エンコーディング タイプを識別します。
compress	メッセージ本文を UNIX ファイル圧縮を使用して転送する転送エンコーディング タイプを識別します。
default	トラフィックが設定されたリストにないサポートされる要求方式を含む場合にセキュリティ アプライアンスが実行するデフォルトのアクションを指定します。
deflate	メッセージ本文を zlib 形式（RFC 1950）とデフレート圧縮（RFC 1951）を使用して転送する転送エンコーディング タイプを識別します。
drop	接続を閉じます。
gzip	メッセージ本文を GNU zip（RFC 1952）を使用して転送する転送エンコーディング タイプを識別します。
identity	転送エンコーディングが実行されていないメッセージ本文の接続を識別します。
log	（任意）syslog を生成します。
reset	TCP リセット メッセージをクライアントおよびサーバに送信します。
type	HTTP アプリケーション インスペクションを通じて制御される転送エンコーディングのタイプを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。コマンドがイネーブルで、サポートされる転送エンコーディング タイプが指定されていない場合、デフォルト アクションでは、ロギングなしで接続を許可します。デフォルトのアクションを変更するには、**default** キーワードを使用して、別のデフォルト アクションを指定します。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP 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　**transfer-encoding** コマンドがイネーブルの場合、セキュリティ アプライアンスは、サポートされ設定されている各転送エンコーディング タイプの HTTP 接続に指定されたアクションを適用します。

セキュリティ アプライアンスは、設定されたリストの転送エンコーディング タイプに一致*しない*すべてのトラフィックに**デフォルト**のアクションを適用します。設定済みの**デフォルト**のアクションでは、ロギングなしで接続を**許可**します。

たとえば、設定済みのデフォルトのアクションでは、**drop** と **log** のアクションを伴う 1 つ以上のエンコーディング タイプを指定した場合、セキュリティ アプライアンスは、設定されたエンコーディング タイプを含む接続をドロップし、各接続をロギングし、その他のサポートされるエンコーディング タイプの接続をすべて許可します。

より限定的なポリシーを設定する場合は、デフォルトのアクションを **drop**（または **reset**）と **log**（イベントをロギングする場合）に変更します。その後、許可されたエンコーディング タイプそれぞれに **allow** アクションを設定します。

適用する各設定に対して 1 回ずつ **transfer-encoding** コマンドを入力します。デフォルト アクションを変更するために **transfer-encoding** コマンドの 1 つのインスタンスを使用し、設定された転送エンコーディング タイプのリストに各エンコーディング タイプを追加するために 1 つのインスタンスを使用します。

設定されたアプリケーション タイプのリストからアプリケーション カテゴリを削除するために、このコマンドの **no** 形式を使用する場合は、コマンドラインのアプリケーション カテゴリ キーワードの後ろの文字は無視されます。

例　次に、特に禁止されていないすべてのサポートされるアプリケーション タイプを許可する設定済みのデフォルトを使用して、許可ポリシーを提供する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# transfer-encoding gzip drop log
hostname(config-http-map)#
```

この場合、GNU zip を使用する接続だけがドロップされ、そのイベントがロギングされます。

次に、デフォルト アクションを、接続のリセットと、特に許可されていないすべてのエンコーディング タイプのロギングに変更した、限定的なポリシーを提供する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse identity allow
hostname(config-http-map)#
```

この場合、転送エンコーディングを使用していない接続だけが許可されます。他のサポートされるエンコーディング タイプの HTTP トラフィックを受信した場合は、セキュリティ アプライアンスは接続をリセットして syslog エントリを作成します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP インスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

trust-point

IKE ピアに送信する証明書を識別するトラストポイントの名前を指定するには、トンネル グループ ipsec 属性モードで、**trust-point** コマンドを使用します。トラストポイント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。

trust-point *trust-point-name*

no trust-point *trust-point-name*

構文の説明

trust-point-name	使用するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

例

次に、設定 ipsec コンフィギュレーション モードを開始し、IPSec LAN-to-LAN トンネル グループ 209.165.200.225 の IKE ピアに送信される証明書を識別するためのトラストポイントを設定する例を示します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
```

関連コマンド

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

trustpoint（SSO サーバ）

SAML POST-type SSO サーバに送信される証明書を識別するトラストポイントの名前を指定するには、config-webvpn-sso-saml モードで **trustpoint** コマンドを使用します。トラストポイント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。

trustpoint *trustpoint-name*

no trustpoint *trustpoint-name*

構文の説明

trustpoint-name	使用するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3	このコマンドが追加されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを一度だけ入力すれば、別のサーバでさまざまなセキュアなサービスにアクセスできます。セキュリティ アプライアンスは現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

トラストポイントは、特に認証パスの最初の公開キーを提供するために使用される公開キー証明書をはじめ、検証テストの必要なく有効であることを信頼できる CA 発行の証明書に基づいて、認証局 ID を表します。

例

次に、config-webvpn-sso-saml モードを開始し、SAML POST-type SSO サーバに送信される証明書を識別するトラストポイントに名前を付ける例を示します。

```
hostname(config-webvpn)# sso server
hostname(config-webvpn-sso-saml)# trustpoint mytrustpoint
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント情報を管理します。
show webvpn sso server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso server	SSO サーバのタイプを作成、命名、および指定します。

tsig enforced

TSIG リソース レコードの存在を必須とするには、パラメータ コンフィギュレーション モードで **tsig enforced** 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。

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

構文の説明

drop	TSIG が存在しない場合にパケットをドロップします。
log	システム メッセージ ログを生成します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DNS トランザクションにおける TSIG の存在のモニタと強制をイネーブルにします。

例

次に、DNS インスペクション ポリシー マップ内で TSIG 強制をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tsig enforced action log
```

関連コマンド

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

ttl-evasion-protection

存続可能時間回避保護をディセーブルにするには、tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** 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。

ttl-evasion-protection

no ttl-evasion-protection

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

セキュリティ アプライアンスによって提供される TTL 回避保護は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用して、セキュリティ ポリシーを回避しようとする攻撃を阻止できます。

たとえば、攻撃者は非常に短い TTL を持ち、ポリシーに合致するパケットを送信できます。TTL がゼロになると、セキュリティ アプライアンスとエンドポイントの間のルータはパケットをドロップします。この時点で、攻撃者は TTL を長くした悪意のあるパケットを送信できます。このパケットは、セキュリティ アプライアンスにとって再送信のように見えるため、通過します。一方、エンドポイント ホストにとっては、このパケットが攻撃者によって受信された最初のパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。この機能をイネーブルにすると、このような攻撃を阻止します。

例

次に、ネットワーク 10.0.0.0 から 20.0.0.0 へのフローに対して TTL 回避保護をディセーブルにする例を示します。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# ttl-evasion-protection disable
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

tunnel-group

IPSec および WebVPN トンネルの接続固有のデータベースを作成し管理するには、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを使用します。トンネル グループを削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **type** *type*

no tunnel-group *name*

構文の説明

name	トンネル グループの名前を指定します。任意のストリングを選択できます。名前が IP アドレスの場合は、通常、ピアの IP アドレスとなります。
type	トンネル グループのタイプを指定します。 • remote-access：ユーザに IPSec リモート アクセスまたは WebVPN（ポータルまたはトンネル クライアント）のいずれかを使用した接続を許可します。 • ipsec-l2l：2 つのサイトまたは LAN がインターネットなどのパブリック ネットワークを介してセキュアに接続できる IPsec LAN-to-LAN を指定します。 **（注）** 次のトンネル グループ タイプは、リリース 8.0(2) で廃止されました。 ipsec-ra：IPSec リモート アクセス webvpn：WebVPN セキュリティ アプライアンスはこれらを remote-access タイプに変換します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	「注」を参照してください。	•	—	—

（注） tunnel-group コマンドは、トランスペアレント ファイアウォール モードで使用可能です。このモードでは、LAN-to-LAN トンネル グループのコンフィギュレーションは設定できますが、remote-access グループまたは WebVPN グループの設定はできません。LAN-to-LAN に対応する tunnel-group コマンドはすべてトランスペアレント ファイアウォール モードで使用できます。

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。
7.1(1)	webvpn タイプが追加されました。
8.0(2)	remote-access タイプが追加され、ipsec-ra タイプと webvpn タイプが廃止されました。

使用上のガイドライン

セキュリティ アプライアンスには、次のデフォルト トンネル グループがあります。

- DefaultRAGroup、デフォルトの IPSec remote-access トンネル グループ
- DefaultL2LGroup、デフォルトの IPSec LAN-to-LAN トンネル グループ
- DefaultWEBVPNGroup、デフォルトの WebVPN トンネル グループ

これらのグループは変更できますが、削除はできません。トンネル ネゴシエーションで識別された特定のトンネル グループがない場合は、セキュリティ アプライアンスは、これらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

tunnel-group コマンドを入力した後、適切な後続のコマンドを入力して、特定のトンネル グループの特定の属性を設定できます。これらのコマンドはそれぞれ、トンネル グループ属性を設定するためのコンフィギュレーション モードを開始します。

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

例

次に、グローバル コンフィギュレーション モードを開始する例を示します。最初に、リモート アクセス トンネル グループを設定します。グループ名は group1 です。

```
hostname(config)# tunnel-group group1 type remote-access
hostname(config)#
```

次に、webvpn トンネル グループ「group1」を設定する tunnel-group コマンドの例を示します。このコマンドはグローバル コンフィギュレーション モードで入力します。

```
hostname(config)# tunnel-group group1 type webvpn
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	設定一般モードを開始し、全般的なトンネル グループ属性を設定します。
tunnel-group ipsec-attributes	設定 ipsec モードを開始し、IPSec トンネル グループ属性を設定します。

コマンド	説明
tunnel-group ppp-attributes	L2TP 接続の PPP 設定を行うための設定 ppp モードを開始します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

tunnel-group general-attributes

一般属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group general-attributes** コマンドを使用します。このモードは、すべてのサポートされるトンネリング プロトコルに共通の設定値を設定するために使用されます。

すべての一般属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **general-attributes**

no tunnel-group *name* **general-attributes**

構文の説明

general-attributes	このトンネル グループの属性を指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	他のトンネル グループ タイプのさまざまな属性が、一般トンネル グループ属性リストに移行され、トンネル グループ一般属性モードのプロンプトが変更されました。

例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用してリモート アクセス接続のリモート アクセス トンネル グループを作成し、その後、トンネル グループ一般属性を設定するための一般属性コンフィギュレーション モードを開始する例を示します。トンネル グループの名前は、209.165.200.225 です。

```
hostname(config)# tunnel-group 209.165.200.225 type remote-access
hostname(config)# tunnel-group 209.165.200.225 general-attributes
hostname(config-tunnel-general)#
```

次に、グローバル コンフィギュレーション モードを開始し、IPSec リモート アクセス接続用のトンネル グループ「remotegrp」を作成し、その後、トンネル グループ「remotegrp」の一般属性を設定するための一般コンフィギュレーション モードを開始する例を示します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group ipsec-attributes

ipsec 属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group ipsec-attributes** コマンドを使用します。このモードは、IPSec トンネリング プロトコルに固有の設定値を設定するために使用されます。

すべての IPSec 属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **ipsec-attributes**

no tunnel-group *name* **ipsec-attributes**

構文の説明

ipsec-attributes	このトンネル グループの属性を指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	さまざまな IPSec トンネル グループ属性が一般トンネル グループ属性リストに移行され、トンネル グループ ipsec 属性モードのプロンプトが変更されました。

例

次に、グローバル コンフィギュレーション モードを開始し、IPSec リモート アクセス トンネル グループ remotegrp のトンネル グループを作成し、その後、IPSec グループ属性を指定する例を示します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group ppp-attributes

ppp 属性コンフィギュレーション モードを開始し、IPSec を介した L2TP 接続によって使用される PPP 設定値を設定するには、グローバル コンフィギュレーション モードで **tunnel-group ppp-attributes** コマンドを使用します。

すべての PPP 属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **ppp-attributes**

no tunnel-group *name* **ppp-attributes**

構文の説明

name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

PPP 設定値は Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）によって使用されます。L2TP は、リモート クライアントがダイヤルアップ電話サービスのパブリック IP ネットワークを使用してプライベート社内ネットワーク サーバとセキュアに通信できるようにする VPN トンネリング プロトコルです。L2TP はクライアント/サーバ モデルに基づき、PPP over UDP（ポート 1701）を使用してデータをトンネルします。tunnel-group ppp コマンドはすべて、PPPoE トンネル グループ タイプで使用できます。

例

次に、トンネル グループ *telecommuters* を作成し、ppp 属性コンフィギュレーション モードを開始する例を示します。

```
hostname(config)# tunnel-group telecommuters type pppoe
hostname(config)# tunnel-group telecommuters ppp-attributes
hostname(tunnel-group-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group webvpn-attributes

webvpn 属性コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group webvpn-attributes** コマンドを使用します。このモードでは、WebVPN トンネリングに共通の設定値を設定します。

すべての WebVPN 属性を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* **webvpn-attributes**

no tunnel-group *name* **webvpn-attributes**

構文の説明

webvpn-attributes	このトンネル グループの WebVPN 属性を指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、グローバル コンフィギュレーション モードを開始し、LAN-to-LAN ピアの IP アドレスを使用して WebVPN 接続用のトンネル グループを作成し、その後、WebVPN 属性を設定するための webvpn コンフィギュレーション モードを開始する例を示します。トンネル グループの名前は、209.165.200.225 です。

```
hostname(config)# tunnel-group 209.165.200.225 type webvpn
hostname(config)# tunnel-group 209.165.200.225 webvpn-attributes
hostname(config-tunnel-webvpn)#
```

次に、グローバル コンフィギュレーション モードを開始し、WebVPN 接続用のトンネル グループ「remotegrp」を作成し、その後、トンネル グループ「remotegrp」の WebVPN 属性を設定するための webvpn コンフィギュレーション モードを開始する例を示します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体または指定されたトンネル グループだけをクリアします。
show running-config tunnel-group	指定されたトンネル グループまたはすべてのトンネル グループの現在実行されているトンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続固有レコードのデータベースを作成および管理します。

tunnel-group-map default-group

tunnel-group-map default-group コマンドでは、他の設定された方式を使用して名前を判別できない場合に使用するデフォルトのトンネル グループを指定します。

tunnel-group-map を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no tunnel-group-map

構文の説明

default-group *tunnel-group-name*	他の設定された方式では名前を取得できない場合に使用するデフォルトのトンネル グループを指定します。*tunnel-group name* はすでに存在している必要があります。
rule index	任意。**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

デフォルト

tunnel-group-map default-group のデフォルト値は DefaultRAGroup です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

証明書からトンネル グループ名を取得する処理は、トンネル グループに関連付けられていない証明書マップのエントリを無視します（どのマップ ルールもこのコマンドでは識別されません）。

例

次の例はグローバル コンフィギュレーション モードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。使用するトンネル グループの名前は group1 です。

```
hostname(config)# tunnel-group-map default-group group1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	暗号 CA 証明書マップ モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map enable	証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーとルールを設定します。

tunnel-group-map enable

tunnel-group-map enable コマンドでは、証明書ベースの IKE セッションをトンネル グループにマッピングするためのポリシーとルールを設定します。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。

tunnel-group-map [*rule-index*] **enable** *policy*

no tunnel-group-map enable [*rule-index*]

構文の説明

policy	証明書からトンネル グループ名を取得するためのポリシーを指定します。*policy* は次のいずれかです。 **ike-id**：トンネル グループがルール ルックアップに基づいて判別されない、または ou から取得されない場合は、フェーズ 1 IKE ID の内容に基づいて証明書ベースの IKE セッションをトンネル グループにマッピングされることを示します。 **ou**：トンネル グループがルール ルックアップに基づいて判別されない場合は、サブジェクト Distinguished Name（DN; 認定者名）の Organizational Unit（OU; 組織ユニット）の値が使用されることを示します。 **peer-ip**：トンネル グループが規則の検索に基づいて決定されないか、ou または ike-id メソッドから取得されない場合、確立されたピア IP アドレスを使用することを示します。 **rules**：このコマンドによって設定された証明書マップ アソシエーションに基づいて、証明書ベースの IKE セッションがトンネル グループにマッピングされることを示します。
rule index	任意。**crypto ca certificate map** コマンドで指定したパラメータを参照します。有効な値は 1 ～ 65535 です。

デフォルト

tunnel-group-map コマンドのデフォルト値は **enable ou** で、**default-group** は DefaultRAGroup に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

crypto ca certificate map コマンドは、証明書マッピング ルールの優先順位リストを保守します。設定できるマップは 1 つだけです。ただし、65535 個までのルールをそのマップに設定できます。詳細については、**crypto ca certificate map** コマンドの資料を参照してください。

例

次に、フェーズ 1 IKE ID の内容に基づく、証明書ベースの IKE セッションとトンネル グループとのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

次に、確立済みのピアの IP アドレスに基づく、証明書ベースの IKE セッションとトンネル グループとのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

次に、サブジェクト Distinguished Name（DN; 認定者名）の Organizational Unit（OU; 組織ユニット）に基づく、証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

次に、確立済みのルールに基づく証明書ベースの IKE セッションのマッピングをイネーブルにする例を示します。

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name（クリプト CA 証明書マップ）	ルール エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルトのトンネル グループとして指定します。

tunnel-limit

セキュリティ アプライアンス上でアクティブになることが許可される GTP トンネルの最大数を指定するには、**gtp-map** コマンドを使用してアクセスする GTP マップ コンフィギュレーション モードで **tunnel limit** コマンドを使用します。トンネル制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

構文の説明

max_tunnels	トンネルの最大許容数です。グローバルなトンネル全体の制限の範囲は、1 ～ 4294967295 です。

デフォルト

トンネル制限のデフォルトは、500 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このコマンドで指定したトンネル数に達すると、新しい要求はドロップされます。

例

次に、GTP トラフィックの最大トンネル数を 10,000 に指定する例を示します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# tunnel-limit 10000
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
debug gtp	GTP インスペクションの詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。

コマンド	説明
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

tx-ring-limit

プライオリティ キューの深さを指定するには、プライオリティ キュー モードで **tx-ring-limit** 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。

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

構文の説明

number-of-packets	イーサネット送信ドライバが許容できる低遅延パケットまたは標準のプライオリティのパケットの最大数を指定します。このパケットの処理が終わると、イーサネット送信ドライバは輻輳が解消するまで、インターフェイス上のパケットをバッファしているキューの処理に戻ります。 **tx-ring-limit** の値の範囲は、PIX プラットフォームでは 3 から 128 パケットで、ASA プラットフォームでは 3 から 256 パケットです。

デフォルト

デフォルトの **tx-ring-limit** は、128 パケットです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

セキュリティ アプライアンスでは、遅延の影響を受けやすい、プライオリティの高いトラフィック（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）と、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）の 2 つのトラフィック クラスを使用できます。セキュリティ アプライアンスは、プライオリティ トラフィックを認識して、適切な Quality of Service（QoS）ポリシーを適用します。プライオリティ キューのサイズと深さを設定して、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にする前に、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューを作成する必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドで、プライオリティ キュー モードを開始します。これ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）、およびパケットをドロップする前にバッファに入れることができる両タイプ（プライオリティまたはベストエフォート）のパケット数（**queue-limit** コマンド）を設定できます。

（注）　インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する*必要があります*。

指定する tx-ring-limit および queue-limit は、プライオリティ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方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの 2 つのパラメータを調整することで、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、実行時にダイナミックに決定されます。この制限を表示するには、コマンド ラインに **help** または **?** と入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。**queue-limit** の値の範囲は、0 ～ 2048 パケットです。**tx-ring-limit** の値の範囲は、PIX プラットフォームでは 3 から 128 パケットで、ASA プラットフォームでは 3 から 256 パケットです。

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

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

例

次の例では、test というインターフェイスにプライオリティ キューを、キュー制限を 2048 パケットに、送信キュー制限を 256 パケットに設定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 2048
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの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。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
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。

コマンド	説明
show priority-queue statistics	指定されたインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config 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** キーワードを指定した場合、このコマンドは、現在の **priority-queue**、**queue-limit**、および **tx-ring-limit** コマンドのコンフィギュレーション値をすべて表示します。

type echo

SLA 動作をエコー応答時間プローブ動作として設定するには、SLA モニタ コンフィギュレーション モードで **type echo** コマンドを使用します。SLA コンフィギュレーションからタイプを削除するには、このコマンドの **no** 形式を使用します。

type echo protocol ipIcmpEcho *target* interface *if-name*

no type echoprotocol ipIcmpEcho *target* interface *if-name*

構文の説明

interface *if-name*	エコー要求パケットを送信するために使用されるインターフェイスのインターフェイス名を、**nameif** コマンドで指定されているとおりに指定します。インターフェイス送信元アドレスが、エコー要求パケットの送信元アドレスとして使用されます。
protocol	プロトコルのキーワード。サポートされる唯一の値が **ipIcmpEcho** で、エコー動作で IP/ICMP エコー要求を使用するように指定します。
target	モニタするオブジェクトの IP アドレスまたはホスト名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

ICMP パケットのペイロードのデフォルト サイズは 28 バイトで、合計サイズが 64 バイトの ICMP パケットを作成します。ペイロード サイズは、**request-data-size** コマンドを使用して変更できます。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。SLA の到達可能性を追跡するために、ID が 1 のトラッキング エントリを作成します。SLA 動作の頻度を 10 秒、しきい値を 2500 ミリ秒、タイムアウト値を 4000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
```

```
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
request-data-size	SLA 動作要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。