CHAPTER 32

tcp-map コマンド～ type echo コマンド

tcp-map

TCP フローの検査をカスタマイズするには、グローバル コンフィギュレーション モードで **tcp-map** コマンドを使用します。TCP マップの指定を削除するには、このコマンドの **no** 形式を使用します。

tcp-map *map_name*

no tcp-map *map_name*

シンタックスの説明

map_name	モジュラ ポリシー CLI モードで TCP マップを適用するために使用する 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用して、高度な TCP 接続設定を設定します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

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 モードに入ります。次のコマンドを tcp マップ コンフィギュレーション モードで使用できます。

check-retransmission	再転送データのチェックをイネーブルおよびディセーブルにします。
checksum-verification	チェックサムの確認をイネーブルおよびディセーブルにします。
exceed-mss	ピアにより設定された MSS を超過した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付けされていないパケットの最大数を設定します。このコマンドは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用できます。PIX 500 シリーズのセキュリティ アプライアンスでは、キューに入れられるパケットは 3 つまでで、この数を変更することはできません。
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り提供された 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して URG ポインタを許可または消去します。
window-variation	突然ウィンドウ サイズが変更された接続をドロップします。

例

次の例では、localmap という名前の TCP マップの使用を指定するための **tcp-map** コマンドの使用方法を示します。

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

hostname(config)# tcp-map localmap

hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

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消去します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
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して TCP オプションを許可または消去するには、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**}

シンタックスの説明

allow	TCP ノーマライザを通して TCP オプションを許可します。
clear	TCP ノーマライザを通して TCP オプションを消去し、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）です。
selective-ack	選択的な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	timestamp オプションを設定します。timestamp オプションを消去すると、PAWS および RTT がディセーブルとなります。デフォルトでは、timestamp 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）です。
window-scale	window scale mechanism オプションを設定します。デフォルトでは、window scale mechanism 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

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 モードに入ります。tcp マップ コンフィギュレーション モードで **tcp-options** コマンドを使用して、selective-acknowledgement オプション、window-scale オプション、および timestamp TCP オプションを消去します。また、明確に定義されていないオプションを持つパケットも消去またはドロップできます。

例

次の例では、TCP オプションが 6 ～ 7 および 9 ～ 255 の範囲にあるすべてのパケットをドロップする方法を示します。

```
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
hostname(config)#
```

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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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 アクセスを追加して、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。あらかじめ設定された 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*}}

シンタックスの説明

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できるホストの名前を指定します。
interface_name	Telnet へのネットワーク 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を認可す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を認可する 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*	Telnet セッションがセキュリティ アプライアンスによって停止されるまでにアイドル状態を維持する時間（分）。有効な値は 1 ～ 1,440 分です。

デフォルト

デフォルトでは、Telnet セッションのアイドル状態が 5 分間続くと、セキュリティ アプライアンスによって停止されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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。また、**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 コマンドでは、Telnet でセキュリティ アプライアンス コンソールにアクセスできるホストを指定できます。セキュリティ アプライアンスへの Telnet 接続は、すべてのインターフェイスでイネーブルにできます。ただし、セキュリティ アプライアンスでは、外部インターフェイスへの Telnet トラフィックがすべて、必ず IPSec で保護されます。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、まず外部インターフェイス上で、IPSec がセキュリティ アプライアンスの生成する IP トラフィックを含むように設定した後、外部インターフェイスで Telnet をイネーブルにします。

no telnet コマンドを使用すると、それまでに設定した IP アドレスから Telnet アクセスが削除されます。**telnet timeout** コマンドを使用すると、コンソールの Telnet セッションの最大アイドル時間を設定して、その時間が経過すると、セキュリティ アプライアンスがログオフするようにできます。**no telnet** コマンドは、**telnet timeout** コマンドと共に使用できません。

IP アドレスを入力した場合、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 マスクを使用しないでください。*netmask* は、IP アドレスのビット マスクだけです。アクセスを IP アドレス 1 つに制限するには、255.255.255.255 のように各オクテットに 255 を使用します。

IPSec が動作中の場合に、アンセキュアなインターフェイス名（通常、外部インターフェイス）を指定できます。**telnet** コマンドでインターフェイス名を指定するには、少なくとも、**crypto map** コマンドを設定する必要があります。

passwd コマンドを使用して、コンソールへの Telnet アクセスで使用するパスワードを設定します。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している IP アドレスを表示します。**kill** コマンドを使用して、アクティブな Telnet コンソール セッションを終了します。

aaa コマンドを **console** キーワードと共に使用する場合は、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）　**aaa** コマンドを設定して、セキュリティ アプライアンス Telnet コンソール アクセスに認証を要求した場合に、コンソール ログイン要求がタイムアウトしたときは、セキュリティ アプライアンス ユーザ名と **enable password** コマンドで設定したパスワードを入力して、シリアル コンソールからセキュリティ アプライアンスにアクセスできます。

例

次の例では、ホスト 192.168.1.3 および 192.168.1.4 が Telnet を通してセキュリティ アプライアンス コンソールへのアクセス許可を得る方法を示します。さらに、192.168.2.0 ネットワーク上のすべてのホストがアクセスを許可されます。

```
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
```

次の例では、セッションの最大アイドル継続時間を変更する方法を示します。

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

次の例では、Telnet コンソール ログイン セッションを示します（パスワードは入力時には表示されません）。

```
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削除することも、すべての telnet コマンド文を clear configure telnet コマンドで削除することもできます。

```
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な 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**}

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、ロギングをイネーブルにしてから、現在のセッションだけでロギングをディセーブルにする方法を示します。

```
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消去します。
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*

シンタックスの説明

[**lines**] *lines*	「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページが無制限であることを示します。範囲は 0 ～ 2,147,483,647 行です。**lines** キーワードはオプションです。このキーワードの有無にかかわらず、コマンドは同じです。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 セッションに対してだけ 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 Telnet 接続する場合、ある特定のコンテキスト内の **pager** コマンドに異なる設定があっても、他のコンテキストに移ったときには、pager line 設定はユーザのセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次の例では、表示される行数を 20 に変更します。

```
hostname# 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消去します。
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	システム ログ メッセージが Telnet セッションで表示されるようにします。
terminal width	グローバル コンフィギュレーション モードで端末の表示幅を設定します。

terminal width

コンソール セッション中に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***

シンタックスの説明

columns	端末の幅をカラム単位で指定します。デフォルトは 80 です。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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、端末の表示幅を 100 カラムにする方法を示します。

```
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消去します。
show running-config terminal	現在の端末設定を表示します。
terminal	特権 EXEC モードで端末回線のパラメータを設定します。

test aaa-server

test aaa-server コマンドを使用して、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します。AAA サーバへの到達に失敗する場合、セキュリティ アプライアンスのコンフィギュレーションが誤っているか、他の理由（ネットワーク コンフィギュレーションまたはサーバのダウンタイムが制限されているなど）で到達不能になっている可能性があります。

test aaa-server {authentication | authorization} *server-tag* **[host** *server-ip*] **[username** *username*] **[password** *password*]

シンタックスの説明

authentication	セキュリティ アプライアンスはテスト認証要求を送信する必要があることを指定します。
authorization	セキュリティ アプライアンスはテスト認可要求を送信する必要があることを指定します。
host *server-ip*	AAA サーバの IP アドレスを指定します。
password *password*	所定のユーザ名のパスワードを指定します。**password** 引数は認証テストの場合にだけ使用できます。入力されたユーザ名に対してパスワードが正しいことを確認します。正しくない場合、認証テストは失敗します。
server-tag	**aaa-server protocol** コマンドで定義されているサーバ グループの識別名を指定します。
username *username*	AAA サーバ設定のテストに使用されるアカウントのユーザ名を指定します。AAA サーバ上にそのユーザ名が存在することを確認します。存在しない場合、テストは失敗します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
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 コマンドを使用して、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します。このコマンドを使用すると、実際のサプリカントでテストする必要がないため、セキュリティ アプライアンス上のコンフィギュレーションの確認が簡略化されます。また、認証および認可の失敗が、AAA サーバ パラメータの設定の誤り、AAA サーバへの接続の問題、またはセキュリティ アプライアンスでのその他のコンフィギュレーション エラーに起因するものかどうかを識別できます。

このコマンドを入力すると、***host*** および ***password*** キーワードと引数のペアを省略できます。セキュリティ アプライアンスは、これらの値を入力するようにプロンプトを表示します。認証テストを実行している場合、***password*** キーワードと引数のペアを省略して、セキュリティ アプライアンスがプロンプトを表示しているときにパスワードを入力できます。

例

次の例では、ホスト 192.168.3.4 の srvgrp1 という名前の RADIUS AAA サーバに対して、タイムアウト 9 秒、リトライ間隔 7 秒、認証ポート 1650 を設定します。AAA サーバ パラメータの設定に続く **test aaa-server** コマンドは、認証テストがサーバに到達できずに失敗したことを示しています。

```
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: ******
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Server not responding: No error
```

関連コマンド

コマンド	説明
aaa-server host	特定の AAA サーバのパラメータを指定します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

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*

シンタックスの説明

input_text	正規表現と照合す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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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。

入力したテキストと正規表現が一致すると、次のメッセージが表示されます。

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

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

次の例は、入力したテキストと正規表現が一致するかどうかをテストします。

```
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検査クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数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	アプリケーション検査のため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。これは CA SiteMinder コマンドによる SSO です。

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

シンタックスの説明

server-name	テストされる SSO サーバの名前を指定します。
user-name	テストされる SSO サーバ上のユーザ名を指定します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**test sso-server** コマンドは、SSO サーバが認識されるかどうか、および認証要求に応答するかどうかをテストします。

server-name 引数により指定された SSO サーバが検出されない場合は、次のエラーが表示されます。

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

SSO サーバが検出されても *user-name* 引数によって指定されたユーザが検出されない場合、認証は拒否されます。

例

特権 EXEC モードで入力された次の例では、my-sso-server という名前の SSO サーバが Anyuser というユーザ名を使用して正常にテストされています。

```
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#
```

次の例は同じサーバのテストを示していますが、Anyuser というユーザ名は認識されず、認証は失敗しています。

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

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

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

シンタックスの説明

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 番目の色が黒の場合、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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、タイトルバーのテキストの色を黒に設定する方法を示します。

```
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 2 番目の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 サーバおよびパスと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 アドレスと IPv6 アドレスをサポートしています。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

シンタックスの説明

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、このインターフェイスがアンセキュアな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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	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** コマンドや **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、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	コンフィギュレーションを TFTP サーバ上の指定パスからロードします。
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。

threshold

SLA 監視オペレーションのしきい値超過イベントを決める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

シンタックスの説明

milliseconds	宣言する上限値をミリ秒で指定します。有効な値は 0 ～ 2147483647 です。ただし、タイムアウトに設定された値よりも大きな値にすることはできません。

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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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だけに使われます。このイベントは、到達可能性には影響しませんが、**timeout** コマンドの設定が正しいかどうかを調べるために使用できます。

例

次の例では、ID が 123 の SLA オペレーションを設定し、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 オペレーションの頻度を 10 秒、しきい値を 2,500 ミリ秒、タイムアウト値を 4,000 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 監視オペレーションを定義します。
timeout	SLA オペレーションが応答を待機する期間を定義します。

timeout

アイドル状態の最大継続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。

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

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

シンタックスの説明

absolute	（オプション）タイムアウトになった場合は、無条件に再認証を求めます。
conn	（オプション）接続が終了するまでのアイドル時間を指定します。最短時間は 5 分です。
hh:*mm*:*ss*	タイムアウト時間を指定します。
h225 *hh*:*mm*:*ss*	（オプション）H.225 シグナリング接続が終了するまでのアイドル時間を指定します。
h323	（オプション）H.245（TCP）および H.323（UDP）メディア接続が終了するまでのアイドル時間を指定します。デフォルトは 5 分です。 **（注）** H.245 および H.323 メディア接続の両方に同じ接続フラグが設定されるため、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	（オプション）TCP ハーフクローズ接続が解放されるまでのアイドル時間を指定します。
icmp	（オプション）ICMP のアイドル時間を指定します。
inactivity	（オプション）無活動タイムアウトになった場合は、再認証を求めます。
mgcp *hh:mm:ss*	（オプション）MGCP メディア接続が削除されるまでのアイドル時間を指定します。
mgcp-pat *hh:mm:ss*	（オプション）MGCP PAT 変換が削除されるまでの絶対間隔を設定します。
rpc	（オプション）RPC 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。最短時間は 1 分です。
sip	（オプション）SIP タイマーを修正します。
sip-disconnect	（オプション）メディアが削除され、メディア xlate が終了するまでのアイドル時間を設定します。範囲は 1 ～ 10 分です。デフォルトは 2 分です。
sip-invite	（オプション）暫定応答のピンホールおよびメディア xlate が終了するまでのアイドル時間を設定します。範囲は 1 ～ 30 分です。デフォルトは 3 分です。
sip_media	（オプション）SIP メディア タイマーを修正します。メディア タイマーは、UDP 非アクティビティ タイムアウトの代わりに、SIP UDP メディア パケットを扱う SIP RTP/RTCP で使用されます。
sunrpc	（オプション）SUNRPC スロットが終了するまでアイドル時間を指定します。
uauth	（オプション）認証および認可キャッシュがタイムアウトするまでの継続時間を設定します。ユーザは次回の接続時に再認証を必要とします。
udp	（オプション）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。最短時間は 1 分です。
xlate	（オプション）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。最短時間は 1 分です。

デフォルト

デフォルトは次のとおりです。

- **conn** *hh*:*mm*:*ss* は、1 時間（**01:00:00**）です。
- **h225** *hh*:*mm*:*ss* は、1 時間（**01:00:00**）です。
- **h323** *hh*:*mm*:*ss* は、5 分（**00:05:00**）です。
- **half-closed** *hh*:*mm*:*ss* は、10 分（**00:10:00**）です。
- **icmp** *hh:mm:ss* は、2 分（**00:00:0***2*）です。
- **mgcp** *hh:mm:ss* は、5 分（**00:05:00**）です。
- **mgcp-pat** *hh:mm:ss* は、5 分（**00:05:00**）です。
- **rpc** *hh*:*mm*:*ss* は、10 分（**00:10:00**）です。
- **sip** *hh:mm:* は、30 分（**00:30:00**）です。
- **sip-disconnect** *hh:mm:ss* は、2 分（**00:02:00**）です。
- **sip-invite** *hh:mm:ss* は、3 分（**00:03:00**）です。
- **sip_media** *hh:mm:ss* は、2 分（**00:02:00**）です。
- **sunrpc** *hh:mm:ss* は、10 分（**00:10:00**）です。
- **uauth** *hh:mm:ss* は、5 分（**00:5:00 absolute**）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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	キーワード ***mgcp-pat***、**sip-disconnect**、および **sip-invite** が追加されました。

使用上のガイドライン

timeout コマンドは、接続、変換 UDP、および RPC の各スロットに許容されるアイドル時間を設定します。指定されたアイドル時間内に、そのスロットが使用されていなければ、リソースがフリープールに戻されます。TCP 接続スロットは、通常の接続終了シーケンスの約 60 秒後に解放されます。

（注） 接続に受動 FTP を使用している場合、または Web 認証に **virtual** コマンドを使用している場合は、**timeout uauth 0:0:0** コマンドは使用しないでください。

timeout コマンドの後ろにキーワードと値を複数入力できます。

接続タイマーは、変換タイマーに優先します。つまり、変換タイマーは、すべての接続がタイムアウトした後に初めて動作します。

conn *hh*:*mm*:*ss* を設定する場合、**0:0:0** を使用すると、接続がタイムアウトしません。

half-closed *hh*:*mm*:*ss* を設定する場合、**0:0:0** を使用すると、ハーフクローズ接続がタイムアウトしません。

h255 *hh*:*mm*:*ss* を設定する場合、**h225 00:00:00** を使用すると、H.225 シグナリング接続が絶対に終了しません。タイムアウト値を **h225 00:00:01** に設定すると、タイマーがディセーブルになり、すべてのコールが消去された後、TCP 接続がすぐに終了します。

uauth *hh*:*mm*:*ss* 時間は、**xlate** キーワード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。接続上で受動 FTP が使用されている場合は、0 には設定しないでください。

absolute キーワードをディセーブルにするには、uauth タイマーに 0（ゼロ）を設定します。

例

次の例では、アイドル状態の最大継続時間を設定する方法を示します。

```
hostname(config)# timeout uauth 0:5:00 absolute uauth 0:4:00 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
show running-config timeout	指定し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 サーバとの接続の確立を中止するまでの、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て、タイムアウト時間をデフォルト値の 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

シンタックスの説明

seconds	要求に対するタイムアウト間隔（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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(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 タイプに有効です。

timeout コマンドを使用して、セキュリティ アプライアンスが AAA サーバへの接続を試みる時間の長さを指定します。**retry-interval** コマンドを使用して、セキュリティ アプライアンスが接続を試行する間隔を指定します。

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に必要となる合計所要時間です。リトライ間隔は、タイムアウト期間中に通信が再試行される頻度を決定します。したがって、リトライ間隔がタイムアウト値以上の場合、再試行されません。再試行する場合は、リトライ間隔をタイムアウト値よりも小さくする必要があります。

例

次の例では、ホスト 1.2.3.4 上の「svrgrp1」という名前の RADIUS AAA サーバに、タイムアウト値 30 秒、リトライ間隔 10 秒を設定します。したがって、セキュリティ アプライアンスは、30 秒後に中止するまで通信を 3 度試行します。

```
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 モードに入って、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 コマンド文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 サーバを試すまで待機する時間を指定するには、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*]

シンタックスの説明

seconds	タイムアウトを 1 ～ 30 の間の秒単位で指定します。デフォルトは 2 秒です。セキュリティ アプライアンスが一連のサーバを試すたびに、このタイムアウトは倍増します。再試行の回数を設定するには、dns サーバ グループ コンフィギュレーション モードで **retries** コマンドを使用します。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

例

次の例では、DNS サーバ グループの「dnsgroup1」に対してタイムアウトを 1 秒に設定しています。

```
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	ユーザが作成したすべての DNS サーバ グループを削除して、デフォルトのサーバ グループのアトリビュート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。
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、一連の DNS サーバへのアクセス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 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ビティ タイマーを変更するには、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。このモードには、**gtp-map** コマンドを使用してアクセスできます。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*

シンタックスの説明

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 が削除されるまでの非アクティビティの継続時間を指定します。
pdp-context	PDP コンテキストの受信を開始するまでの、許可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までの､許可される最大時間を指定します。
signaling	GTP シグナリングが削除されるまでの非アクティビティの継続時間を指定します。
t3-response	GTP 接続が削除されるまでに応答を待つ最長時間を指定します。
tunnel	GTP トンネルが終了するまでの非アクティビティの継続時間を指定します。

デフォルト

デフォルトは、**gsn**、**pdp-context**、および **signaling** に対して 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（Delete PDP Context Request を受信していない場合）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	No

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 の組み合せであるトンネル識別子（TID）によって識別されます。各 MS は最大 15 の NSAPI を持つことができ、様々な QoS レベルのアプリケーション要件に基づいて、それぞれが異なる NSAPI を持つ複数の PDP コンテキストを作成できます。

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

例

次の例では、要求キューに対して 2 分のタイムアウト値を設定します。

```
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 GTP 統計情報を消去します。
debug gtp	GTP 検査に関する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	アプリケーション検査に使用する特定の 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 アカウンティングのユーザの非アクティビティ タイマーを変更するには、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。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。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*

シンタックスの説明

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値を指定します。

デフォルト

ユーザのデフォルトのタイムアウト値は 1 時間です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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	•	•	•	•	No

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ユーザのタイムアウト値を 10 分に設定します。

```
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検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

timeout（SLA モニタ）

SLA オペレーションで要求パケットへの応答を待つ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

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

SLA オペレーションで要求パケットを送信する頻度を設定するには **frequency** コマンドを使用し、要求への応答を受信するために待機時間を設定するには **timeout** コマンドを使用します。**timeout** コマンドで指定する値は、**frequency** コマンドで指定する値より大きくすることはできません。

例

次の例では、ID が 123 の SLA オペレーションを設定し、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 オペレーションの頻度を 10 秒、しきい値を 2,500 ミリ秒、タイムアウト値を 4,000 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 オペレーションを繰り返す頻度を指定します。
sla monitor	SLA 監視オペレーションを定義します。

timeout pinhole

DCERPC ピンホールのタイムアウト値を設定し、グローバルなシステム ピンホール タイムアウト値である 2 分を上書きするには、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

シンタックスの説明

hh:mm:ss	ピンホール接続のタイムアウト値。0:0:1 ～ 1193:0:0 の値を指定できます。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、DCERPC 検査ポリシー マップのピンホール接続のタイムアウト値を設定する方法を示します。

```
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 マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

time-range

時間範囲コンフィギュレーション モードに入り、トラフィックの規則、またはアクションに関連付ける時間範囲を定義するには、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*

シンタックスの説明

name	時間範囲の名前。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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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、時間範囲だけを定義します。時間範囲を定義したら、トラフィックの規則かアクションに関連付けます。

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** コマンドと共に使用して、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 クロックによって決まりますが、NTP で同期を取れます。

例

次の例では、New_York_Minute という時間範囲を作成し、時間範囲コンフィギュレーション モードに入ります。

```
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 モードに入ったら、**absolute** キーワードと **periodic** キーワードを使用して時間範囲のパラメータを定義できます。***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードの設定をデフォルトに戻すには、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。次に、**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。次の例では、Sales という ACL を New_York_Minute という時間範囲にバインドします。

```
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	時間範囲が有効である絶対時間を定義します。
access-list extended	セキュリティ アプライアンス経由の 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*** キーワードの設定をデフォルトに戻します。
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。

timers spf

最短パス優先（SPF）計算の遅延時間と待機時間を指定するには、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*]

シンタックスの説明

delay	OSPF によるトポロジ変更の受信と最短パス優先（SPF）計算の開始との間の遅延時間（1 ～ 65,535 秒）を指定します。
holdtime	2 つの連続した SPF 計算の間の待機時間（秒）で、有効な値は 1 ～ 65,535 秒です。

デフォルト

デフォルトは次のとおりです。

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

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF プロトコルによるトポロジ変更受信と計算開始との間の遅延時間、および 2 つの連続した SPF 計算での待機時間を設定するには、**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

次の例では、SPF 計算の遅延時間に 10 秒、SPF 計算の待機時間に 20 秒を設定します。

```
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 モードに入ります。
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 リンクステート アドバタイズメント（LSA）が収集されてリフレッシュ、チェックサム、またはエージングされ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するときに WebVPN のページに表示される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*

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

シンタックスの説明

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

デフォルト

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の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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

タイトルを入れない場合は、*value* の引数なしで **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現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

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

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。

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

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

例

次の例では、タイトルを「Cisco WebVPN Service」というテキストでカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(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）パラメータを使用して WebVPN ページをカスタマイズします。

tos

SLA オペレーションの要求パケットの IP ヘッダーでタイプ オブ サービス（ToS）バイトを定義するには、SLS 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

シンタックスの説明

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

デフォルトは 0 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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、優先度、信頼性などの情報が入っています。ネットワークにある他のルータのポリシー ルーティングや、専用アクセス レートなどの機能で使用されます。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。また、エコー要求パケットのペイロード サイズを 48 バイト、SLA オペレーション中に送信するエコー要求の数を 5、タイプ オブ サービス バイトを 80 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)# 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 オペレーション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 監視オペレーションを定義します。
type echo	SLA オペレーションをエコー応答時間プローブ オペレーションとして設定します。

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***]

シンタックスの説明

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*** コマンドを使用して定義するか、DNS サーバを設定して traceroute がホスト名を IP アドレスに名前解決できるようにします。www.example.com などの DNS ドメイン名がサポートされています。
source	トレース パケットの送信元となる 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 トレースの送信元の IP アドレスを指定します。この IP アドレスは、送信元インターフェイスの IP アドレスでなければなりません。透過モードでは、セキュリティ アプライアンスの管理 IP アドレスを指定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。指定した場合は、送信元のインターフェイスの IP アドレスが使用されます。
numeric	このコマンドの出力に、中間のゲートウェイの IP アドレスだけが表示されるようにします。このキーワードを指定しないと、トレース中に到達したゲートウェイのホスト名が検索されます。
timeout	使用するタイムアウト値を指定します。
timeout_value	接続がタイムアウトになるまでに、応答を待つ時間を秒単位で指定します。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。デフォルトは 3 です。
ttl	プローブで使用する Time To Live（TTL; 存続可能時間）の範囲を指定するキーワード。
min_ttl	最初のプローブの TTL の値。デフォルトは 1 ですが、高い値に設定して、既知のホップが表示されないようにすることもできます。
max-ttl	使用できる TTL の最大値。デフォルトは 30 です。トレースするパケットが宛先に到達するか、TTL がこの値になるとコマンドは終了します。
port *port_value*	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）プローブ メッセージで使用する宛先ポート。デフォルトは 33434 です。
use-icmp	UDP プローブ パケットではなく、ICMP プローブ パケットを使用することを指定します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

traceroute コマンドは、送信された各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、このコマンドの出力で使われる記号を示します。

出力に示される記号	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 のホストに到達できません。
!P	ICMP プロトコルが見つかりません。
!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

次の例では、traceroute コマンドで宛先 IP アドレスを指定した場合の出力を示します。

```
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	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。
packet-tracer	パケットのトレース機能をイネーブルにします。

track rtr

SLA オペレーションの到達可能性を調べるには、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 のトラッキングを削除するには、このコマンドの **no** 形式を使用します。

track *track-id* ***rtr*** *sla-id* ***reachability***

no track *track-id* ***rtr*** *sla-id* ***reachability***

シンタックスの説明

reachability	オブジェクトの到達可能性を追跡することを指定します。
sla-id	トラッキング エントリで使用する SLA の ID。
track-id	トラッキング エントリのオブジェクト ID を作成します。有効な値は 1 ～ 500 です。

デフォルト

SLA のトラッキングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(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 コマンドで、トラッキング エントリのオブジェクト ID を作成し、そのエントリで使用する SLA を指定します。

SLA オペレーションごとに、オペレーション戻りコード値が保持されます。この値は、トラッキング プロセスで解釈されます。OK、Over Threshold、および他のいくつかの戻りコードがあります。表 32-1 に、戻りコードが意味するオブジェクトの到達可能性の状態を示します。

表 32-1　SLA トラッキングの戻りコード

トラッキング	戻りコード	トラッキング状態
到達可能性	OK または Over Threshold	アップ
	その他のコード	ダウン

例

次の例では、ID が 123 の SLA オペレーションを設定し、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 監視オペレーションを定義します。

traffic-non-sip

既知の SIP シグナリング ポートを使用して SIP 以外の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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップで、既知の SIP シグナリング ポートを使用した SIP 以外のトラフィックを許可する方法を示します。

```
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 マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

transfer-encoding

転送符号化タイプを指定することで HTTP トラフィックを制限するには、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。このモードには、**http-map** コマンドを使用してアクセスできます。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。

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***]

シンタックスの説明

action	指定した転送符号化タイプを使用している接続が検出された場合に実行され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	メッセージ本文が一連のチャンクとして転送される転送符号化タイプを識別します。
compress	UNIX ファイル圧縮を使用してメッセージ本文が転送される転送符号化タイプを識別します。
default	サポートされている要求メソッドがトラフィックに含まれていて、そのメソッドが設定済みリストに記載されていない場合に、セキュリティ アプライアンスが実行するデフォルト アクションを指定します。
deflate	zlib 形式（RFC 1950）およびデフレート圧縮（RFC 1951）を使用して、メッセージ本文が転送される転送符号化タイプを識別します。
drop	接続を終了します。
gzip	GNU zip（RFC 1952）を使用してメッセージ本文が転送される転送符号化タイプを識別します。
identity	転送符号化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	（オプション）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またはサーバに送信します。
type	HTTP アプリケーション検査を通して制御される転送符号化タイプを指定します。

デフォルト

このコマンドは、デフォルトでは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符号化タイプが指定されていない場合、デフォルトのアクションは接続をロギングなしで許可します。デフォルト 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 コマンドをイネーブルにする場合、セキュリティ アプライアンスは、サポートおよび設定された各転送符号化タイプの HTTP 接続に、指定し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、設定したリストの転送符号化タイプに一致*しない*すべてのトラフィックに、**default** アクションを適用します。事前設定済みの **default** アクションでは、接続をロギングなしで **allow** します。

たとえば、事前設定済みのデフォルトのアクションが与えられ、**drop** および **log** のアクションを伴う符号化タイプを 1 つ以上指定する場合、セキュリティ アプライアンスは設定済みの符号化タイプを含む接続をドロップして、各接続のログを記録し、サポートされるその他の符号化タイプに対してすべての接続を許可します。

より厳しいポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log** に変更します（イベントをログに記録する場合）。次に、**allow** アクションを使用して、許容される符号化タイプをそれぞれ設定します。

適用する各設定に対して、**transfer-encoding** コマンドを 1 度入力します。**transfer-encoding** コマンドの 1 つのインスタンスはデフォルト アクションの変更に使用し、もう 1 つのインスタンスは設定済みの転送符号化タイプのリストに各符号化タイプを追加するために使用します。

このコマンドの **no** 形式を使用して、設定済みのアプリケーション 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場合は、アプリケーション カテゴリのキーワードの後ろに入力した文字がすべて無視されます。

例

次の例では、事前設定済みのデフォルトを使用して、緩やかなポリシーを指定しています。サポートされているすべてのアプリケーション タイプを、個別に拒否されていない限り許可します。

```
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 を使用した接続だけがドロップされ、イベントのログが記録されます。

次の例では、特に許可されていない任意の符号化タイプに対し、接続をリセットしてイベントをログに記録するようにデフォルト アクションを変更した厳しいポリシーを指定します。

```
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、転送符号化を使用していない接続だけが許可されます。サポートされるその他の符号化タイプの HTTP トラフィックを受信した場合、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先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

trust-point

IKE ピア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、トンネル グループ IPSec アトリビュート モードで **trust-point** コマンドを使用します。トラストポイント仕様を削除するには、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*

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

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

例

次の例は config-ipsec コンフィギュレーション モードで入力され、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループの IKE ペアに送られる証明書を識別するためのトラストポイントを設定します。

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

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

tsig enforced

TSIG リソース レコードを必須とするには、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**}]

シンタックスの説明

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、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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いて、TSIG の監視をイネーブルにし、TSIG が必ず存在することを要求します。

例

次の例では、DNS 検査ポリシー マップで TSIG 強制をイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

ttl-evasion-protection

Time-To-Live 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

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

セキュリティ アプライアンスが提供する 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

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 モードに入ります。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した攻撃を防止します。

たとえば、攻撃者は非常に短い TTL を持つポリシーを通過するパケットを送信できます。TTL が 0 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。攻撃者は、この時点で長い TTL を持つ悪意のあるパケットを送信できます。セキュリティ アプライアンスはこのパケットを再送と見なし、通過させます。ただし、エンドポイントのホストでは、このパケットが攻撃者より受信した最初のパケットとなります。このような場合、攻撃者は攻撃を防ぐセキュリティがなくても成功します。この機能をイネーブルにすると、このような攻撃を防ぐことができます。

例

次の例では、ネットワーク 10.0.0.0 から 20.0.0.0 へのフローで TTL 回避保護をディセーブルにする方法を示します。

```
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（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、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 トンネルに対する接続固有のレコード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*

シンタックスの説明

name	トンネル グループの名前を指定します。これには、任意の文字列を選択できます。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次のように指定します。 ipsec-ra：IPSec リモートアクセス ipsec-l2l：IPsec LAN-to-LAN webvpn：WebVPN

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

（注）　tunnel-group コマンドは、透過ファイアウォール モードで使用して、LAN-to-LAN トンネル グループのコンフィギュレーションを許可できますが、リモートアクセス グループまたは WebVPN グループは許可できません。また、LAN-to-LAN で使用できるすべての tunnel-group コマンドは、透過ファイアウォール モードでも使用できます。

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.1	webvpn タイプが追加されました。

使用上のガイドライン

セキュリティ アプライアンスには、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 リモート アクセス 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

これらのグループの変更はできますが、削除はできません。セキュリティ アプライアンスは、トンネル ネゴシエーション中に特定のトンネル グループが識別されない場合、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 グループに対してデフォルトのトンネル パラメータを設定します。

tunnel-group コマンドを入力した後、特定のトンネル グループに特定のアトリビュートを設定するには、次のコマンドから適切なものを入力します。それぞれのコマンドは、トンネル グループ アトリビュートを設定するためのコンフィギュレーション モードに入ります。

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

例

次の例は、グローバル コンフィギュレーション モードで入力されています。最初のコマンドは、IPSec 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 ipsec-ra
hostname(config)#
```

次の例では、IPSec LAN-to-LAN トンネル グループを設定します。名前は、LAN-to-LAN ピアの IP アドレスです。

```
hostname(config)# tunnel-group 209.165.200.225 type ipsec-l2l
hostname(config)#
```

次の例では、「group1」という名前の webvpn トンネル グループを設定する tunnel-group コマンドを示します。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 グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	一般トンネル グループ アトリビュートを設定する config-general モードに入ります。
tunnel-group ipsec-attributes	IPSec トンネル グループ アトリビュートを設定する config-ipsec モードに入ります。
tunnel-group ppp-attributes	L2TP 接続の PPP を設定する config-ppp モードに入ります。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

tunnel-group general-attributes

一般アトリビュート コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **tunnel-group general-attributes** コマンドを使用します。このモードは、サポートされるすべてのトンネリング プロトコルに共通の値を設定するために使用されます。

一般アトリビュートをすべて削除するには、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**

シンタックスの説明

***general*-attributes**	このトンネル グループのアトリビュートを指定します。
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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。
7.1.1	さまざまなアトリビュートが他のトンネル グループ タイプから一般トンネル グループ アトリビュート リストに移され、トンネル グループ一般アトリビュート モードのプロンプトが変更されました。

使用上のガイドライン

次の表は、このグループに属しているコマンドと、コマンドを設定できるトンネル グループのタイプを示しています。

一般アトリビュート	設定できるトンネル グループのタイプ
accounting-server-group	IPSec RA、IPSec L2L、WebVPN
address-pool	IPSec RA
authentication-server-group	IPSec RA、WebVPN
authorization-dn-attributes	IPSec RA、WebVPN
authorization-required	WebVPN
authorization-server-group	IPSec RA
default-group-policy	IPSec RA、IPSec L2L
dhcp-server	IPSec RA
override-account-disabled	IPSec RA、WebVPN
password-management	IPSec RA、WebVPN

一般アトリビュート	設定できるトンネル グループのタイプ
strip-group	IPSec RA、WebVPN
strip-realm	IPSec RA、WebVPN

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、LAN-to-LAN ピアの IP アドレスを使用して IPSec LAN-to-LAN 接続用のトンネル グループを作成してから一般コンフィギュレーション　モードに入り、一般アトリビュートを設定します。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 IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 general
hostname(config-tunnel-general)#
```

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、IPSec リモートアクセス接続用の「remotegrp」という名前のトンネル グループを作成してから一般コンフィギュレーション モードに入り、「remotegrp」という名前のトンネル グループ用の一般アトリビュートを設定します。

```
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、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル 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 トンネルの接続に固有な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 アトリビュート コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **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 プロトコルに限定される値を設定するために使用されます。

IPSec アトリビュートをすべて削除するには、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**

シンタックスの説明

***ipsec*-attributes**	このトンネル グループのアトリビュートを指定します。
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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。
7.1.1	さまざまな IPSec トンネル グループ アトリビュートが一般トンネル グループ アトリビュート リストに移され、トンネル グループ ipsec アトリビュート モードのプロンプトが変更されました。

使用上のガイドライン

次のコマンドは、このグループに所属しています。

IPSec アトリビュート	設定できるトンネル グループのタイプ
chain	IPSec RA、IPSec L2L
client-update	IPSec RA
isakmp keepalive	IPSec RA
peer-id-validate	IPSec RA、IPSec L2L
pre-shared-key	IPSec RA、IPSec L2L
radius-with-expiry	IPSec RA
trust-point	IPSec RA、IPSec L2L

例

次の例はグローバル コンフィギュレーションで入力され、remotegrp という名前の IPSec リモート アクセス トンネル グループ用のトンネル グループを作成してから、IPSec グループ アトリビュートを指定します。

```
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、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル 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 トンネルの接続に固有な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 アトリビュート コンフィギュレーション モードに入り、L2TP over IPSec 接続で使用する PPP 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。

PPP アトリビュートをすべて削除するには、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**

シンタックスの説明

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2.1	このコマンドが導入されました。

使用上のガイドライン

PPP 設定は、Layer 2 Tunneling Protocol（L2TP）で使用されます。これは、リモート クライアントがパブリック IP ネットワークにダイヤルアップ接続して、企業のプライベート ネットワーク サーバと安全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 モデルに基づいており、PPP over UDP（ポート 1701）を使用してデータをトンネリングします。

次の表は、このグループに属しているコマンドと、コマンドを設定できるトンネル グループのタイプを示しています。

PPPoE アトリビュート	設定できるトンネル グループのタイプ
authentication chap	PPPoE
authentication eap-proxy	PPPoE
authentication ms-chap-v1	PPPoE
authentication ms-chap-v2	PPPoE
authentication-pap	PPPoE

例

次の例では、*telecommuters* というトンネル グループを作成し、PPP アトリビュート コンフィギュレーション モードに入ります。

```
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、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル 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 トンネルの接続に固有な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 アトリビュート コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **tunnel-group webvpn-attributes** コマンドを使用します。このモードは WebVPN トンネリングに共通した値を設定します。

WebVPN アトリビュートをすべて削除するには、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**

シンタックスの説明

***webvpn*-attributes**	このトンネル グループの WebVPN アトリビュートを指定します。
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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

一般アトリビュートに加えて、WebVPN 接続に固有の次のアトリビュートを WebVPN アトリビュート モードで設定できます。

- authentication
- customization
- dns-group
- group-alias
- group-url
- hic-fail-group-policy
- nbns-server-name

これらのアトリビュートの設定に関する詳細については、個々のコマンドの説明を参照してください。

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、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 グループを作成してから webvpn コンフィギュレーション モードに入り、WebVPN アトリビュートを設定します。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、WebVPN 接続用の「remotegrp」という名前のトンネル グループを作成してから webvpn コンフィギュレーション モードに入り、「remotegrp」という名前のトンネル グループ用の WebVPN アトリビュートを設定します。

```
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、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル 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 トンネルの接続に固有な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 コマンドは、他の設定済みの方法でトンネル グループ名を判別できなかった場合に、使用するデフォルトのトンネル グループ名を指定します。

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*

シンタックスの説明

default-group *tunnel-group-name*	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。*tunnel-group name* は、既存である必要があります。
rule index	オプション。**crypto ca certificate map** コマンドで指定したパラメータを参照します。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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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ポリシーと規則を設定します。**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、証明書マッピング規則の優先順位付きリストを管理します。定義できるマップは 1 つのみです。ただし、このマップで 65,535 個までの規則を保持できます。詳細については、**crypto ca certificate map** コマンドのマニュアル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（どのマップ規則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	crypto ca 証明書マップ モードに入ります。
subject-name（暗号 CA 証明書マップ）	規則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 グループにマップするポリシーと規則を設定します。

tunnel-group-map enable

tunnel-group-map enable 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ポリシーと規則を設定します。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*]

シンタックスの説明

policy	証明書からトンネル グループ名を取得するポリシーを指定します。*policy* は、次のいずれかになります。 **ike-id**：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、または ou から取得されない場合、証明書ベースの IKE セッションはフェーズ 1 IKE ID のコンテンツに基づいたトンネル グループにマップされることを示します。 **ou**：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場合、サブジェクト認定者名（DN）の組織ユニット（OU）の値を使用することを示します。 **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**：証明書ベースの IKE セッションは、このコマンドにより設定された証明書マップ結合に基づいてトンネル グループにマップされることを示します。
rule index	オプション。**crypto ca certificate map** コマンドで指定したパラメータを参照します。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　次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　**crypto ca certificate map** コマンドは、証明書マッピング規則の優先順位付きリストを管理します。定義できるマップは 1 つのみです。ただし、このマップで 65,535 個までの規則を保持できます。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

例　次の例では、フェーズ 1 IKE ID のコンテンツに基づいて、トンネル グループへの証明書ベースの IKE セッションのマッピングをイネーブルにします。

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

次の例では、確立されたピアの IP アドレスに基づいて、トンネル グループへの証明書ベースの IKE セッションのマッピングをイネーブルにします。

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

次の例では、サブジェクト認定者名（DN）の組織ユニット（OU）に基づいて証明書ベースの IKE セッションのマッピングをイネーブルにします。

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

次の例では、確立した規則に基づいて、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 モードに入ります。
subject-name（暗号 CA 証明書マップ）	規則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 トンネル グループとして指定します。

tunnel-limit

セキュリティ アプライアンスでアクティブになることを許可されている GTP トンネルの最大数を指定するには、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。このモードには、**gtp-map** コマンドを使用してアクセスできます。トンネル制限をデフォルトに戻すには、**no** を使用します。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

シンタックスの説明

max_tunnels	これは、トンネルの許容最大数です。グローバルなトンネル制限全体の範囲は、1 ～ 4,294,967,295 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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定されたトンネル数に到達すると、新しい要求はドロップされます。

例

次の例では、GTP トラフィックに最大 10,000 トンネルを指定します。

```
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 GTP 統計情報を消去します。
debug gtp	GTP 検査に関する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	アプリケーション検査に使用する特定の 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 キューの項目数を指定するには、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*

シンタックスの説明

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優先順位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** 値の範囲は、PIX プラットフォームでは 3 ～ 128 パケット、ASA プラットフォームでは 3 ～ 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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プライオリティ 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 アプライアンスは、2 つのクラスのトラフィックを許可します。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティ キューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

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

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

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。**queue-limit** 値の範囲は、0 ～ 2,048 パケットです。**tx-ring-limit** 値の範囲は、PIX プラットフォームでは 3 ～ 128 パケット、ASA プラットフォームでは 3 ～ 256 パケットです。

例

次の例では、test というインターフェイスのプライオリティ キューを設定して、キューの上限を 2048 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 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。
show priority-queue statistics	指定し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** キーワードを指定すると、このコマンドは現在のすべての **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表示します。

type echo

SLA オペレーションをエコー応答時間プローブ オペレーション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。このタイプのオペレーションを SLA コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

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

no type echo ***protocol ipIcmpEcho*** *target* interface *if-name*

シンタックスの説明

interface *if-name*	**nameif** コマンドで指定したように、エコー要求パケットを送信するインターフェイスの名前を指定します。インターフェイスの送信元アドレスが、エコー要求パケットで送信元アドレスとして使用されます。
protocol	プロトコルを指定するキーワード。***ipIcmpEcho*** という値しか指定できません。この値は、エコー オペレーションで IP/ICMP エコー要求を使用することを指定します。
target	監視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

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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 バイトです。ICMP パケットの合計サイズは 64 バイトになります。ペイロードのサイズを変更するには、**request-data-size** コマンドを使用します。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。ID が 1 のトラッキング エントリを作成し、SLA の到達可能性を追跡します。SLA オペレーションの頻度を 10 秒、しきい値を 2,500 ミリ秒、タイムアウト値を 4,000 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 オペレーション中に送信する要求パケットの数を指定します。
request-data-size	SLA オペレーションの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 監視オペレーションを定義します。