T ～ Z のコマンド

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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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ともに使用して、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。
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
```

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 オプションをクリアにすると、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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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ともに使用します。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 の範囲で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
```

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。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
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。

コマンドのモード

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
7.0	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

端末回線のパラメータを設定するには、特権 EXEC モードで **terminal** コマンドを使用します。

terminal {**monitor** | **no monitor** | **pager lines** [*lines*]}

シンタックスの説明

monitor	この端末での syslog メッセージの表示をイネーブルにします。
no monitor	この端末での syslog メッセージの表示をディセーブルにします。
pager 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。

デフォルト

lines の引数が指定されていない場合、***terminal monitor pager*** のデフォルトは 24 行です。

コマンドのモード

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
7.0	***pager lines*** コマンドが追加されました。

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。
show running-config terminal	現在の端末設定を表示します。
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。

コマンドのモード

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
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のみ使用できます。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。

コマンドのモード

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
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。

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。

コマンドのモード

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
7.0	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 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。

コマンドのモード

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
7.0	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** コマンドの入力が簡略化されます。**configure net** コマンドまたは **write net** コマンドを入力する場合、**tftp-server** コマンドで指定した TFTP サーバを継承することも、独自の値を入力することもできます。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。

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_media** | **uauth** *hh*:*mm*:*ss*]

シンタックスの説明

conn	（オプション）経過後に接続を終了する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）経過後に H.225 シグナリング接続が終了するアイドル時間を指定します。
h323	（オプション）経過後に H.245（TCP）および H.323（UDP）メディア接続が終了する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）経過後に TCP ハーフクローズ接続が解放される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。
mgcp *hh:mm:ss*	（オプション）経過後に MGCP メディア接続が削除されるアイドル時間を指定します。
mgcp-pat *hh:mm:ss*	（オプション）経過後に MGCP PAT 変換が削除される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_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）経過後に SUNRPC スロットが終了する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_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** タイマーは、**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。

コマンドのモード

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
7.0	キーワード ***mgcp-pat*** 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。

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、すべてのコールがクリアされた後、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-server host)

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。これは、セキュリティ アプライアンスがプライマリ AAA サーバへの要求を中止するまでの時間です。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスはバックアップ サーバに要求を送信します。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、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)# exit
hostname(config)#
```

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 (gtp-map)

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。これは、**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** | ***tunnel*** } *hh:mm:ss*

no timeout {**gsn** | ***pdp-context*** | ***request*** | **signaling** | ***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。
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 分です（Delete PDP Context Request が受信されていない場合）。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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用に特定の 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。

time-range

時間範囲コンフィギュレーション モードに入り、トラフィック規則または動作に添付でき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	時間範囲の名前です。名前は、64 文字以内である必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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、これをトラフィック規則または動作に添付できます。

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。**access-list extended time-range** コマンドとともに使用して、ACL に時間範囲をバインドします。

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

次の例では、「New_York_Minute」という名前の時間範囲を作成し、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)#
```

時間範囲を作成して、時間範囲コンフィギュレーション モードに入った後、**absolute** コマンドおよび **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*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元するには、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。**access-list extended** コマンドとともに使用して、ACL に時間範囲をバインドします。次の例では、「Sales」という名前の ACL を「New_York_Minute」という名前の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 アプライアンスを通して IP トラフィックの許可または拒否に対するポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードに対するデフォルトの設定を復元します。
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 lsa-group-pacing

OSPF link-state advertisement（LSA; リンクステート アドバタイズメント）がグループに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*]

シンタックスの説明

seconds	OSPF リンクステート アドバタイズメント（LSA）がグループに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です。有効な値は 10 ～ 1,800 秒です。

デフォルト

デフォルトの間隔は 240 秒です。

コマンドのモード

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
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 リンクステート アドバタイズメント（LSA）がグループに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

次の例では、LSA のグループ処理間隔に 500 秒を設定します。

```
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 spf	最短パス優先（SPF）計算の遅延時間と保持時間を指定します。

timers spf

最短パス優先（SPF）計算の遅延時間と保持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 計算の間の保持時間（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。

コマンドのモード

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
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 計算での保持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 計算の保持時間に 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

ブラウザおよび WebVPN タイトルバーに表示される WebVPN ユーザ用のタイトルを設定するには、WebVPN モードで **title** コマンドを使用します。タイトル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。

title [*string*]

no title

シンタックスの説明

string	（オプション）ブラウザ タイトルおよび WebVPN タイトルバーの HTML 文字列を指定します。最大 255 文字です。

デフォルト

デフォルトのタイトルは「WebVPN Service」です。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

タイトルを入れない場合、文字列なしで **title** コマンドを使用します。

例

次の例では、WebVPN タイトル「Our Company WebVPN Services」を作成する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# title Our Company WebVPN Services
```

title-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 タイトルバーの色を設定するには、WebVPN モードで **title-color** コマンドを使用します。タイトル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。

title-color {*color*}

no title-color

シンタックスの説明

color	（オプション）色を指定します。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。 • 名前の長さは、最大で 32 文字です。

デフォルト

デフォルトのタイトルは、HTML の #999CC（薄紫色）です。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

HTML および RGB 値を使用する場合、推奨値は 216 です。推奨色は、数学的にあり得る数よりはるかに少なくなります。多くのディスプレイは 256 色しか処理できず、その中の 40 色は、Macintosh と PC では別の色が表示されます。最適な表示結果を得るには、各所で公開されている HTML および RGB テーブルを確認してください。テーブルをオンラインで見つけるには、検索エンジンで RGB と入力します。

例

次の例では、RGB の色値 153, 204, 255（スカイブルー）を設定する方法を示します。

```
hostname(config)# webvpn

hostname(config-webvpn)# title-color 153,204,255
```

関連コマンド

コマンド	説明
secondary-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 タイトルバーに 2 番目の色を設定します。

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。これは、**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	クライアントまたはサーバに TCP リセット メッセージを送信します。
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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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対して、**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廃棄して、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、アプリケーション カテゴリ キーワード以降、コマンドラインに入力された文字は無視されます。

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)# exit
```

この場合、GNU zip を使用した接続だけが廃棄され、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)# exit
```

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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

すべてのトンネルグループ タイプにこのアトリビュートを適用できます。

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-ipsec)# trust-point mytrustpoint
hostname(config-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。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。
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コンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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ともに使用します。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廃棄します。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みなし、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（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。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
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 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

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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）　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
7.0	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスには、デフォルトで 2 つのトンネルグループがあります。DefaultRAGroup は、デフォルトの IPSec リモートアクセス トンネルグループで、DefaultL2Lgroup は、デフォルトの IPSec LAN-to-LAN トンネルグループです。これらは変更できますが、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 コマンドには、次のコマンドがあります。これらの各コマンドを使用すると、コンフィギュレーション モードのレベルでアトリビュートを設定するコンフィギュレーション モードに入ることができます。

- **tunnel-group general-attributes**
- **tunnel-group ipsec-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、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)#
```

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 map	**crypto ca certificate map** コマンドで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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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
address-pool	IPSec RA
authentication-server-group	IPSec RA
authorization-server-group	IPSec RA
default-group-policy	IPSec RA、IPSec L2L
dhcp-server	IPSec RA
strip-group	IPSec RA
strip-realm	IPSec RA

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-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-general)
```

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（crypto ca certificate map）	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-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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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
authorization-dn-attributes	IPSec RA
authorization-required	IPSec RA
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-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-map default-group	**crypto ca certificate map** コマンドで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ます。

tunnel-group-map default-group

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。

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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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（crypto ca certificate map）	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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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（crypto ca certificate map）	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。これは、**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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定されたトンネル数に到達すると、新しい要求は廃棄されます。

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用に特定の 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。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

セキュリティ 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）用の低遅延キューイング（LLQ）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、プライオリティ トラフィックを認識し、適切な Quality of Service（QoS）ポリシーを強制します。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） インターフェイスに対してプライオリティ 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。

urgent-flag

TCP ノーマライザを通して URG ポインタ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 **urgent-flag** 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。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

シンタックスの説明

allow	TCP ノーマライザを通して URG ポインタを許可します。
clear	TCP ノーマライザを通して URG ポインタを消去します。

デフォルト

緊急フラグおよび緊急オフセットはデフォルトで消去されます。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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ともに使用します。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 **urgent-flag** コマンドを使用して、緊急フラグを許可します。

URG フラグは、ストリーム内の他のデータよりも高い優先順位の情報を含むパケットを示すために使用されます。TCP RFC は、URG フラグの正確な解釈を明確化していません。したがって、エンド システムは緊急オフセットをさまざまな方法で処理します。このため、エンド システムが攻撃を受け易くなります。デフォルトの動作は、URG フラグとオフセットを消去します。

例

次の例では、緊急フラグを許可する方法を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 513
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。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
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。

url

CRL を検索するためのスタティック URL のリストを維持するには、crl 設定コンフィギュレーション モードで **url** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。既存の URL を削除するには、このコマンドの **no** 形式を使用します。

url *index url*

no url *index url*

シンタックスの説明

Index	リスト内の各 URL のランクを決定する 1 ～ 5 の値を指定します。セキュリティ アプライアンスは、インデックス 1 から URL を試行します。
url	CRL の検索元となる URL 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。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずそれを削除して、このコマンドの **no** 形式を使用します。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL 検索用の URL のリストを作成し、維持するためにインデックス 3 を設定して、CRL の検索元となる URL https://foobin.com を設定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://foobin.com
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
policy	CRL の検索元を指定します。

url-block

フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理するには、**url-block** コマンドを使用します。この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。

url-block block *block_buffer_limit*

no url-block block *block_buffer_limit*

Websense 専用

url-block url-mempool *memory_pool_size*

no url-block url-mempool *memory_pool_siz*

シンタックスの説明

block *block_buffer_limit*	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答を保存する HTTP 応答バッファを作成します。許容される値は 0 ～ 128 です。これは、1,550 バイトのブロック数を指定します。
url-mempool *memory_pool_size*	Websense URL フィルタリングのみ。URL バッファ メモリ プールのサイズ（KB 単位）。許容される値は、2 ～ 10,240 で、2 KB ～ 10,240 KB の URL バッファ メモリ プールを指定します。
url-size *long_url_size*	Websense URL フィルタリングのみ。最大許容 URL サイズ（KB 単位）。許容される値は、2、3、または 4 で、最大 URL サイズ 2 KB、3 KB、または 4KB 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。

コマンドのモード

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
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

Websense フィルタリング サーバの場合、**url-block url-size** コマンドを使用すると、最大 4 KB の長さの URL のフィルタリングが可能です。Websense フィルタリング サーバおよび N2H2 フィルタリング サーバの両方の場合、**url-block block** コマンドは、URL フィルタリング サーバからの応答を待つ間の Web クライアント要求に応じて Web サーバから受信したパケットをセキュリティ アプライアンスにバッファします。この処理により、デフォルトのセキュリティ アプライアンスの動作と比較して、Web クライアントのパフォーマンスが改善されます。デフォルトの動作はパケットを廃棄し、接続が許可された場合は Web サーバにパケットの再転送を要求します。

url-block block コマンドを使用し、フィルタリング サーバが接続を許可した場合、セキュリティ アプライアンスは、HTTP 応答バッファから Web クライアントにブロックを送信して、バッファからブロックを削除します。フィルタリング サーバが接続を拒否した場合、セキュリティ アプライアンスは拒否メッセージを Web クライアントに送信して、HTTP 応答バッファからブロックを削除します。

url-block block コマンドを使用して、フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答のバッファリングに使用するブロックの数を指定します。

url-block url-mempool コマンドとともに **url-block url-size** コマンドを使用して、Websense フィルタリング サーバによりフィルタリングされる URL の最大長と、URL バッファに割り当てる最大メモリを指定します。これらのコマンドを使用して、1,159 バイト以上 4,096 バイト以下の URL を Websense サーバに渡します。**url-block url-size** コマンドは、1,159 バイトより長い URL をバッファに保存した後、その URL を Websense サーバに渡します（TCP パケット ストリームを使用して）。その結果、Websense サーバがその URL へのアクセスを許可または拒否できます。

例

次の例では、1,550 バイトのブロックを 56 個、URL フィルタリング サーバからの応答のバッファリングに割り当てます。

```
hostname#(config)# url-block block 56
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタをクリアします。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

url-cache

N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにして、キャッシュのサイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。この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。

url-cache {**dst** | **src_dst**} *kbytes* **[kb]**

no url-cache {**dst** | **src_dst**} *kbytes* **[kb]**

シンタックスの説明

dst	URL 宛先アドレスに基づくキャッシュ エントリ。このモードは、N2H2 サーバまたは Websense サーバ上で、すべてのユーザが同じ URL フィルタリング ポリシーを共有する場合に選択します。
size *kbytes*	キャッシュ サイズの値を 1 ～ 128 KB の範囲で指定します。
src_dst	URL 要求を発信している送信元アドレスと URL 宛先アドレスの両方に基づくキャッシュ エントリ。このモードは、N2H2 サーバまたは Websense サーバ上で、ユーザが同じ URL フィルタリング ポリシーを共有していない場合に選択します。
statistics	**statistics** オプションを使用すると、追加の URL キャッシュ統計情報、たとえば、キャッシュ ルックアップの回数やヒット率が表示されます。

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。

コマンドのモード

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
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

url-cache コマンドには、Web サーバからの応答が N2H2 または Websense フィルタリング サービス サーバからの応答よりも高速な場合、Web サーバからの応答をバッファリングするコンフィギュレーション オプションが用意されています。このオプションによって、Web サーバの応答が 2 回ロードされることがなくなります。

url-cache コマンドは、URL キャッシュをイネーブルにし、キャッシュ サイズを設定し、キャッシュの統計情報を表示する場合に使用します。

キャッシュによって URL アクセス特権が、セキュリティ アプライアンス上のメモリに保存されます。ホストが接続を要求すると、セキュリティ アプライアンスは要求を N2H2 または Websense サーバに転送するのではなく、まず一致するアクセス特権を URL キャッシュ内で探します。キャッシュをディセーブルにするには、**no url-cache** コマンドを使用します。

（注）　N2H2 サーバまたは Websense サーバで設定を変更した場合は、**no url-cache** コマンドでキャッシュをディセーブルにした後、**url-cache** コマンドで再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル Version 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル Version 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティの要求に合致する使用状況プロファイルを取得した後、**url-cache** をイネーブルにしてスループットを向上させます。Websense プロトコル Version 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログがアップデートされます。

例

次の例では、送信元アドレスと宛先アドレスに基づいて、すべての発信 HTTP 接続をキャッシュします。

```
hostname(config)# url-cache src_dst 128
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

url-list

WebVPN ユーザがアクセスする URL のセットを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。複数の URL でリストを設定するには、各 URL に対して 1 回、同じリスト名でこのコマンドを複数回使用します。設定済みリスト全体を削除するには、**no url-list** *listname* コマンドを使用します。設定済み URL を削除するには、**no url-list** *listname url* コマンドを使用します。

複数のリストを設定するには、このコマンドを複数回使用して、各リストに一意な *listname* を割り当てます。

url-list {*listname displayname url*}

no url-list *listname*

no url-list *listname url*

シンタックスの説明

displayname	WebVPN エンド ユーザ インターフェイスに表示されるテキストを入力して、URL を識別します。最大 64 文字です。*displayname* は、所定のリストに対して一意である必要があります。スペースを使用できます。
listname	WebVPN ユーザがアクセスできる URL のセットをグループ化します。最大 64 文字です。最大 64 文字です。セミコロン（;）、アンパサンド（&）、小なり（<）記号は使用できません。
url	リンクを指定します。サポートされる URL タイプは http、https、および cifs です。

デフォルト

デフォルトの URL リストはありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで url-list コマンドを使用して、URL のリストを 1 つ以上作成します。特定のグループポリシーまたはユーザがリスト内の URL にアクセスできるようにするには、ここで作成した *listname* とともに WebVPN モードで **url-list** コマンドを使用します。

例

次の例では、www.cisco.com、www.example.com、および www.example.org へのアクセスを提供する *Marketing URLs* という名前の URL リストを作成する方法を示します。次の表は、各アプリケーションの例で使用する値を示します。

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

関連コマンド

コマンド	説明
clear configuration url-list	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
url-list	WebVPN モードでこのコマンドを使用すると、グループポリシーまたはユーザが URL の設定済みリストにアクセスできます。
show running-configuration url-list	現在設定されている URL のセットを表示します。
webvpn	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

url-list (webvpn)

WebVPN サーバのリストと URL を特定のユーザまたはグループポリシーに適用するには、グループポリシーまたはユーザ名モードから入る WebVPN モードで **url-list** コマンドを使用します。**url-list none** コマンドを使用して作成したヌル値を含むリストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを使用します。コマンドを 2 回使用すると、先行する設定値が上書きされます。

url-list {value *name* | **none**}

no url-list

シンタックスの説明

value *name*	URL の設定済みリストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。
none	URL リストにヌル値を設定します。デフォルトのグループポリシーまたは指定されているグループポリシーからリストを継承しないようにします。

デフォルト

デフォルトの URL リストはありません。

コマンドのモード

次の表は、このコマンドを入力するモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

コマンドを 2 回使用すると、先行する設定値が上書きされます。

WebVPN モードで **url-list** コマンドを使用して、ユーザまたはグループポリシー用の WebVPN ホームページに表示する URL リストを識別する前に、リストを作成する必要があります。グローバル コンフィギュレーション モードで **url-list** コマンドを使用して、1 つ以上のリストを作成します。

例

次の例では、FirstGroup という名前のグループポリシーの FirstGroupURL と呼ばれる URL リストの設定方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs
```

関連コマンド

コマンド	説明
clear configure url-list [*listname***]**	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
show running-configuration url-list	現在設定されている **url-list** コマンドのセットを表示します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定するには、グローバル コンフィギュレーション モードでアクセスできる WebVPN モードでこのコマンドを使用します。
webvpn	グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードでアクセスできる WebVPN モードに入り、特定のグループポリシーまたはユーザに対する WebVPN の値を設定します。

url-server

filter コマンドで使用する N2H2 または Websense サーバを指定するには、**url-server** コマンドを使用します。この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。

N2H2

url-server (*if_name***) vendor n2h2 host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*]}]

no url-server (*if_name***) vendor n2h2 host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*]}]

Websense

url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

シンタックスの説明

N2H2

connections	許容する接続の最大数を制限します。
num_conns	許容する接続の最大数を指定します。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	（オプション）認証サーバが常駐するネットワーク インターフェイス。指定しない場合、デフォルトは内部インターフェイスです。
port *number*	N2H2 サーバ ポート。セキュリティ アプライアンスは、UDP 返答のリスンもこのポート上で行います。デフォルトのポート番号は 4005 です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP です。
timeout *seconds*	許容される最大アイドル時間で、経過後にセキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは、30 秒です。
vendor n2h2	URL フィルタリング サービス ベンダーが N2H2 であることを示します。

Websense

connections	許容する接続の最大数を制限します。
if_name	認証サーバが常駐するネットワーク インターフェイス。指定しない場合、デフォルトは内部インターフェイスです。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
timeout *seconds*	許容される最大アイドル時間で、経過後にセキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは、30 秒です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP プロトコル、Version 1 です。
vendor websense	URL フィルタリング サービス ベンダーが Websense であることを示します。
version	プロトコル Version **1** または Version **4** を指定します。デフォルトは TCP プロトコル Version 1 です。TCP は、Version 1 または Version 4 を使用して設定できます。UDP の設定に使用できるのは、Version 4 だけです。

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。

コマンドのモード

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
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

url-server コマンドでは、N2H2 または Websense URL フィルタリング アプリケーションを実行しているサーバを指定します。URL サーバ数の上限は 16 ですが、一度に使用できるアプリケーションは、N2H2 または Websense のどちらか 1 つだけです。さらに、セキュリティ アプライアンス上でコンフィギュレーションを変更しても、アプリケーション サーバ上のコンフィギュレーションはアップデートされないため、ベンダーの指示に従って別途アップデートする必要があります。

HTTPS および FTP に対して **filter** コマンドを実行するには、事前に **url-server** コマンドを設定する必要があります。すべての URL サーバがサーバ リストから削除されると、URL フィルタリングに関連する **filter** コマンドもすべて削除されます。

サーバを指示した後、**filter url** コマンドを使用して、URL フィルタリング サービスをイネーブルにします。

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　ベンダー固有の **url-server** コマンドを適切な形式で使用して、URL フィルタリング アプリケーション サーバを指示します。

ステップ 2　**filter** コマンドで、URL フィルタリングをイネーブルにします。

ステップ 3　（オプション）**url-cache** コマンドを使用して、URL キャッシュをイネーブルにし、認識される応答時間を改善します。

ステップ 4　（オプション）**url-block** コマンドを使用して、長い URL および HTTP のバッファリングのサポートをイネーブルにします。

ステップ 5　**show url-block block statistics**、**show url-cache statistics**、または **show url-server statistics** の各コマンドを使用して、実行情報を表示します。

N2H2 によるフィルタリングの詳細については、次の N2H2 の Web サイトを参照してください。

http://www.n2h2.com

Websense フィルタリングの詳細については、次の Web サイトを参照してください。

http://www.websense.com/

例

次の例では、N2H2 を使用している場合に、10.0.2.54 ホストからの接続を除く、発信 HTTP 接続をすべてフィルタリングします。

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次の例では、Websense を使用している場合に、10.0.2.54 ホストからの接続を除く、発信 HTTP 接続をすべてフィルタリングします。

```
hostname(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
filter url	トラフィックを URL フィルタリング サーバに誘導します。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

user-authentication

ユーザ認証をイネーブルにするには、グループポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication disable** コマンドを使用します。ユーザ認証アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、ユーザ認証の値を別のグループポリシーから継承できます。

イネーブルの場合、ユーザ認証ではハードウェア クライアントの背後にいる個々のユーザが、トンネルを越えてネットワークへのアクセスを取得するように認証する必要があります。

user-authentication {**enable | disable**}

no user-authentication

シンタックスの説明

disable	ユーザ認証をディセーブルにします。
enable	ユーザ認証をイネーブルにします。

デフォルト

ユーザ認証はディセーブルです。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

個々のユーザは設定した認証サーバの順序に従って認証します。

プライマリ セキュリティ アプライアンスでのユーザ認証が必要な場合は、バックアップ サーバでも同様に設定されていることを確認します。

例

次の例では、「FirstGroup」という名前のグループポリシーのユーザ認証をイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を受けずに IP 電話を接続できるようにします。Secure Unit Authentication は有効なままになります。
leap-bypass	イネーブルの場合、LEAP パケットが VPN クライアントの背後にある無線デバイスから VPN トンネルを通過した後でユーザ認証を行ないます。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。
secure-unit-authentication	クライアントがトンネルを開始するたびに VPN クライアントがユーザ名とパスワードを使用した認証を要求することにより、さらにセキュリティが向上します。
user-authentication-idle-timeout	個々のユーザのアイドル タイムアウトを設定します。アイドル タイムアウト期間中にユーザ接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

user-authentication-idle-timeout

ハードウェア クライアントの背後にいる個々のユーザに対してアイドル タイムアウトを設定するには、グループポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを使用します。アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、アイドル タイムアウト値を別のグループポリシーから継承できます。アイドル タイムアウト値を継承しないようにするには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間中にハードウェア クライアントの背後にいるユーザによる通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

シンタックスの説明

minutes	アイドル タイムアウト期間を分単位で指定します。範囲は、1 ～ 35,791,394 分です。
none	無制限のアイドル タイムアウト期間を許容します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーからユーザ認証のアイドル タイムアウト値を継承しないようにします。

デフォルト

30 分。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

例

次の例では、「FirstGroup」という名前のグループポリシーに対して 45 分のアイドル タイムアウト値を設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

username

セキュリティ アプライアンス データベースにユーザを追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名で、このコマンドの **no** バージョンを使用します。すべてのユーザ名を削除するには、ユーザ名を付加せずに、このコマンドの **no** バージョンを使用します。

username {*name*} {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

no username [*name*]

シンタックスの説明

encrypted	パスワードが暗号化されることを示します。
name	ユーザの名前を指定します。
nopassword	このユーザにはパスワードが不要であることを示します。
password *password*	このユーザにはパスワードがあり、パスワードを入力することを示します。
privilege *priv_level*	このユーザに対して特権レベルを設定します。範囲は 0 ～ 15 です。数値が小さくなるほど、コマンドを使用する機能と、セキュリティ アプライアンスを管理する機能が低くなります。デフォルトの特権レベルは 2 です。システム管理者の一般的な特権レベルは 15 です。

デフォルト

デフォルトでは、このコマンドを使用して追加した VPN ユーザには、アトリビュートまたはグループポリシーのアソシエーションはありません。すべての値を明示的に設定する必要があります。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。login コマンドは、このデータベースを認証用に使用します。

例

次の例では、暗号化されたパスワード 12345678 と特権レベル 12 を持つ anyuser という名前のユーザを設定する方法を示します。

```
hostname(config)# username anyuser password 12345678 encrypted privilege 12
```

関連コマンド

コマンド	説明
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションを消去します。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名アトリビュート モードに入って、個々のユーザの AVP を設定できるようにします。

username attributes

ユーザ名アトリビュート モードに入るには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザのすべてのアトリビュートを削除するには、このコマンドの **no** 形式を使用して、ユーザ名を付加します。すべてのユーザのアトリビュートを削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。アトリビュート モードを使用すると、指定したユーザに対して AVP を設定できます。

username {*name*} **attributes**

no username [*name*] **attributes**

シンタックスの説明

name	ユーザ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。

コマンドのモード

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
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。login コマンドは、このデータベースを認証用に使用します。

アトリビュート モードのコマンドのシンタックスには、共通する次の特性があります。

- **no** 形式は、実行コンフィギュレーションからアトリビュートを削除します。
- **none** キーワードも、実行コンフィギュレーションからアトリビュートを削除します。ただし、アトリビュートにヌル値を設定することにより削除され、継承しないようにします。
- ブール アトリビュートには、イネーブルまたはディセーブルになっている設定のための明示的なシンタックスがあります。

例

次の例では、anyuser という名前のユーザのユーザ名アトリビュート コンフィギュレーション モードに入る方法を示します。

```
hostname(config)# username anyuser attributes
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースを消去します。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。

username-prompt

WebVPN に初めてログインする場合のユーザ名のプロンプトを設定するには、WebVPN モードで **username-prompt** コマンドを使用します。デフォルトの「Login:」に戻すには、このコマンドの **no** 形式を使用します。

username-prompt [*prompt*]

no **username-prompt**

シンタックスの説明

prompt	（オプション）ユーザ名を入力するようにユーザに要求する文字列を指定します。最大 16 文字です。

デフォルト

デフォルトのプロンプトは「Login:」です。

コマンドのモード

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
7.0	このコマンドが導入されました。

例

次の例では、パスワード プロンプト「Enter Username:」を設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# password-prompt Enter Username:
```

virtual http

仮想 HTTP サーバを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバ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。セキュリティ アプライアンス上で HTTP 認証を使用し、HTTP サーバも認証を要求している場合、このコマンドを使用すると、セキュリティ アプライアンスと HTTP サーバで別々に認証を実行できます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

シンタックスの説明

ip_address	セキュリティ アプライアンス上の仮想 HTTP サーバに対して IP アドレスを設定します。このアドレスが、セキュリティ アプライアンスに向かってルーティングされる未使用アドレスであることを確認してください。たとえば、外部にアクセスするときに内部アドレスの NAT を実行し、仮想 HTTP サーバへの外部アクセスを提供する場合は、仮想 HTTP サーバ アドレスに対して、グローバル NAT アドレスの 1 つを使用できます。
warning	（オプション）HTTP 接続をセキュリティ アプライアンスにリダイレクトする必要があることをユーザに通知します。このキーワードは、リダイレクトが自動的には行われないテキストベースのブラウザにだけ利用できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

HTTP 認証をイネーブルにする場合（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、セキュリティ アプライアンスは、AAA サーバで認証できるようにユーザ名とパスワードの入力を各ユーザに要求します。AAA サーバがユーザを認証すると、HTTP サーバへの接続が許可されます。ただし、AAA サーバのユーザ名とパスワードは、HTTP パケット内にまだ含まれています。HTTP サーバにも独自の認証メカニズムがある場合、パケットにはすでにユーザ名とパスワードが含まれているため、ユーザが再度ユーザ名とパスワードの入力を要求されることはありません。AAA サーバと HTTP サーバでユーザ名とパスワードが異なる場合、HTTP 認証は失敗します。

HTTP サーバごとに別々に入力を要求できるようにするには、**virtual http** コマンドを使用して、セキュリティ アプライアンスで仮想 HTTP サーバをイネーブルにします。このコマンドは、AAA 認証を必要とするすべての HTTP 接続を、セキュリティ アプライアンス上の仮想 HTTP サーバへリダイレクトします。セキュリティ アプライアンスは、AAA サーバのユーザ名とパスワードを要求します。AAA サーバがユーザを認証すると、セキュリティ アプライアンスは HTTP 接続を元のサーバにリダイレクトしますが、AAA サーバのユーザ名とパスワードは含まれません。HTTP パケットにユーザ名とパスワードが含まれないため、HTTP サーバは別に HTTP サーバのユーザ名とパスワードの入力をユーザに要求します。

注意　**virtual http** コマンドを使用するときは、**timeout uauth** コマンドの継続時間を 0 秒以外に設定します。この設定によって、実際の Web サーバへの HTTP 接続ができなくなります。

例

次の例では、AAA 認証とともに仮想 HTTP をイネーブルにする方法を示します。

```
hostname(config)# access-list HTTP-ACL extended permit tcp 10.1.1.0 any eq 80
hostname(config)# aaa authentication match HTTP-ACL inside tacacs+
hostname(config)# virtual http 10.1.2.1
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド文を削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。
sysopt uauth allow-http-cache	**virtual http** コマンドをイネーブルにすると、このコマンドにより、ブラウザ キャッシュのユーザ名とパスワードを使用して、仮想サーバに再接続できます。
virtual telnet	セキュリティ アプライアンスで仮想 Telnet サーバを提供して、認証を必要とする別のタイプの接続を開始する前に、セキュリティ アプライアンスでユーザを認証できます。

virtual telnet

セキュリティ アプライアンスで仮想 Telnet サーバを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。セキュリティ アプライアンスが認証プロンプトを指定しない別のタイプのトラフィックを認証する必要がある場合、仮想 Telnet サーバでユーザを認証する必要がある場合もあります。サーバ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。

virtual telnet *ip-address*

no virtual telnet *ip-address*

シンタックスの説明

ip_address	セキュリティ アプライアンス上の仮想 Telnet サーバの IP アドレスを設定します。このアドレスが、セキュリティ アプライアンスに向かってルーティングされる未使用アドレスであることを確認してください。たとえば、外部にアクセスするときに内部アドレスの NAT を実行し、仮想 Telnet サーバへの外部アクセスを提供する場合は、仮想 Telnet サーバ アドレスに対して、グローバル NAT アドレスの 1 つを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

任意のプロトコルまたはサービス（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）に対してネットワーク アクセス認証を設定できますが、直接 HTTP、Telnet、または FTP だけで認証することもできます。ユーザは認証を必要とする別のトラフィックが許可される前に、これらのサービスの 1 つで先に認証する必要があります。セキュリティ アプライアンスを通して HTTP、Telnet、または FTP を許可せずに、別のタイプのトラフィックを認証する場合は、セキュリティ アプライアンスで設定された所定の IP アドレスにユーザが Telnet 接続し、セキュリティ アプライアンスが Telnet プロンプトを表示するように、仮想 Telnet を設定できます。

権限のないユーザが仮想 Telnet IP アドレスに接続したとき、ユーザ名とパスワードが要求され、AAA サーバによって認証されます。認証されると、「Authentication Successful.」というメッセージが表示されます。その後、ユーザは認証を必要とするその他のサービスに正常にアクセスできるようになります。

例

次の例では、他のサービスに対する AAA 認証とともに仮想 Telnet をイネーブルにする方法を示します。

```
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 10.1.2.1 eq
telnet
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 209.165.200.225
eq smtp
hostname(config)# aaa authentication match AUTH inside tacacs+
hostname(config)# virtual telnet 10.1.2.1
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド文を削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンス上で HTTP 認証を使用し、HTTP サーバも認証を要求している場合、このコマンドを使用すると、セキュリティ アプライアンスと HTTP サーバで別々に認証を実行できます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。

vlan

VLAN ID をサブインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。サブインターフェイスには、トラフィックを渡す VLAN ID が必要です。VLAN サブインターフェイスを使用すると、1 つの物理インターフェイスに複数の論理インターフェイスを設定できます。VLAN を使用すると、所定の物理インターフェイス（たとえば複数のセキュリティ コンテキスト）にトラフィックを別に保存できます。

vlan *id*

no vlan

シンタックスの説明

id	1 ～ 4,094 の整数を指定します。一部の VLAN ID には、接続されたスイッチで予約されているものもあります。詳細については、スイッチのマニュアル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。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

1 つの VLAN だけを、物理インターフェイスではなく、サブインターフェイスに割り当てることができます。各サブインターフェイスは、トラフィックを通過する前に VLAN ID を持つ必要があります。VLAN ID を変更するには、**no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を使用して **vlan** コマンドを入力でき、セキュリティ アプライアンスは古い ID を変更します。

no shutdown コマンドを使用して物理インターフェイスをイネーブルにし、サブインターフェイスをイネーブルにする必要があります。サブインターフェイスをイネーブルにする場合、物理インターフェイスはタグの付かないパケットを通過させるため、一般的には物理インターフェイスがトラフィックを通過させないようにします。したがって、インターフェイスを停止することで物理インターフェイスを介してトラフィックが通過しないようにすることはできません。代わりに、**nameif** コマンドを省略することで、物理インターフェイスがトラフィックを通過させないことを確認します。物理インターフェイスがタグの付かないパケットを通過させるようにする場合は、通常通り **nameif** コマンドを設定できます。

サブインターフェイスの最大数は、プラットフォームによって変わります。プラットフォームごとの最大サブインターフェイスについては、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例では、サブインターフェイスに VLAN 101 を割り当てます。

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、VLAN を 102 に変更します。

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show running-config interface	インターフェイスの現在のコンフィギュレーションを表示します。

vpn-access-hours

設定済みの時間範囲ポリシーをグループポリシーに関連付けるには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-access-hours** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、時間範囲値を別のグループポリシーから継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを使用します。

vpn-access-hours value {*time-range*} | **none**

no vpn-access hours

シンタックスの説明

none	VPN アクセス時間にヌル値を設定することで、時間範囲ポリシーを許可しないようにします。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。
time-range	設定済みの時間範囲ポリシーの名前を指定します。

デフォルト

無制限です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

例

次の例では、824 と呼ばれる時間範囲ポリシーに FirstGroup という名前のグループポリシーを関連付ける方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

関連コマンド

コマンド	説明
time-range	ネットワークにアクセスする曜日および 1 日の時間を設定します（開始日と終了日を含む）。

vpn-addr-assign

IP アドレスをリモートアクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。設定されている Vpn アドレスの割り当て方法をセキュリティ アプライアンスからすべて削除するには、引数なしで、このコマンドの **no** バージョンを使用します。

vpn-addr-assign {**aaa** | **dhcp** | **local**}

no vpn-addr-assign [**aaa** | **dhcp** | **local**]

シンタックスの説明

aaa	外部 AAA 認証サーバから IP アドレスを取得します。
dhcp	DHCP 経由で IP アドレスを取得します。
local	内部認証サーバから IP アドレスを割り当て、トンネルグループに関連付けます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

DHCP を選択する場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバが使用できる IP アドレスの範囲を定義する必要があります。

ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。**vpn-framed-ip-address** コマンドおよび **vpn-framed-netmask** コマンドを使用して、個々のユーザに IP アドレスとネットマスクを割り当てます。

AAA を選択する場合、設定済みの RADIUS サーバのいずれかから IP アドレスを取得します。

例

次の例では、アドレスの割り当て方法として DHCP を設定する方法を示します。

```
hostname(config)# vpn-addr-assign dhcp
```

関連コマンド

コマンド	説明
dhcp-network-scope	セキュリティ アプライアンス DHCP サーバがグループポリシーのユーザにアドレスを割り当てるときに使用する必要がある IP アドレスの範囲を指定します。
ip-local-pool	ローカル IP アドレス プールを作成します。
vpn-framed-ip-address	IP アドレスを指定して、特定のユーザに割り当てます。
vpn-framed-ip-netmask	ネットマスクを指定して、特定のユーザに割り当てます。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グループポリシーまたはユーザ名モードで **vpn-filter** コマンドを使用します。**vpn-filter none** コマンドを発行して作成したヌル値を含む ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループポリシーから継承できます。値を継承しないようにするには、**vpn-filter none** コマンドを使用します。

ACL を設定して、このユーザまたはグループポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。**vpn-filter** コマンドを使用して、これらの ACL を適用します。

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

シンタックスの説明

none	アクセスリストがないことを指定します。ヌル値を設定して、アクセスリストを拒否します。アクセスリストを他のグループポリシーから継承しないようにします。
value *ACL name*	設定済みアクセスリス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。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

WebVPN は、**vpn-filter** コマンドで定義された ACL を使用しません。

例

次の例では、FirstGroup という名前のグループポリシーの acl_vpn と呼ばれるアクセスリスト名を実行するフィルタを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセスリストを作成します。または、ダウンロード可能なアクセスリストを使用します。

vpn-framed-ip-address

特定のユーザに割り当てる IP アドレスを指定するには、ユーザ名モードで **vpn-framed-ip-address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

シンタックスの説明

ip_address	このユーザの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、anyuser という名前のユーザに 10.92.166.7 という IP アドレスを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

関連コマンド

コマンド	説明
vpn-framed-ip-netmask	このユーザのサブネット マスクを指定します。

vpn-framed-ip-netmask

特定のユーザに割り当てるサブネット マスクを指定するには、ユーザ名モードで **vpn-framed-ip-netmask** コマンドを使用します。サブネットマスクを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-netmask {*netmask*}

no vpn-framed-ip-netmask

シンタックスの説明

netmask	このユーザのサブネット マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、anyuser という名前のユーザに 255.255.255. 254 というサブネット マスクを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
```

（注） RADIUS がサブネット マスクだけを返す場合、認証は独自のサブネット ネットマスクを持つローカル プールからの IP アドレスを使用します。RADIUS からのマスクは使用しません。これを防止するには、RADIUS からネットマスクと IP アドレスの両方を返します。

関連コマンド

コマンド	説明
vpn-framed-ip-address	このユーザの IP アドレスを指定します。

vpn-group-policy

ユーザに設定済みのグループポリシーからアトリビュートを継承させるには、ユーザ名コンフィギュレーション モードで **vpn-group-policy** コマンドを使用します。ユーザ コンフィギュレーションからグループポリシーを削除するには、このコマンドの **no** バージョンを使用します。このコマンドを使用すると、ユーザがユーザ名レベルで設定していないアトリビュートを継承できます。

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

シンタックスの説明

group-policy name	グループポリシーの名前を指定します。

デフォルト

デフォルトでは、VPN ユーザにはグループポリシーのアソシエーションはありません。

コマンドのモード

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
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

アトリビュートをユーザ名モードで利用できる場合、ユーザ名モードで設定することにより、特定のユーザに対するグループポリシーのアトリビュートの値を上書きできます。

例

次の例では、FirstGroup という名前のグループポリシーからアトリビュートを使用するように anyuser という名前のユーザを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループポリシーをセキュリティ アプライアンス データベースに追加します。
group-policy attributes	グループポリシーの AVP を設定できるグループポリシー アトリビュート モードに入ります。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
username attributes	ユーザ名アトリビュート モードに入って、個々のユーザの AVP を設定できるようにします。

vpn-idle-timeout

ユーザのタイムアウト期間を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、タイムアウト値を別のグループポリシーから継承できます。値を継承しないようにするには、**vpn-idle-timeout none** コマンドを使用します。

vpn-idle-timeout {*minutes* | **none**}

no vpn-idle-timeout

シンタックスの説明

minutes	タイムアウト期間を分単位で指定します。1 ～ 35,791,394 の整数を使用します。
none	無制限のアイドル タイムアウト期間を許容します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。

デフォルト

30 分。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、「FirstGroup」という名前のグループポリシーに対して 15 分の VPN アイドル タイムアウトを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

関連コマンド

group-policy	グループポリシーを作成または編集します。
vpn-session-timeout	VPN 接続に許可されている最大時間を設定します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

vpn load-balancing

VPN ロードバランシングおよび関連機能を設定できる VPN ロードバランシング 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 **vpn load-balancing** コマンドを使用します。

vpn load-balancing

（注） ASA Models 5540 および 5520 だけが、VPN ロードバランシングをサポートします。VPN ロードバランシングには、有効な 3DES ライセンスまたは AES ライセンスも必要です。セキュリティ アプライアンスは、ロードバランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。有効な 3DES ライセンスまたは AES ライセンスが検出されなかった場合、セキュリティ アプライアンスはロードバランシングをイネーブルにしません。また、ライセンスで許可されていない限り、ロードバランシング システムが 3DES の内部設定を行わないようにします。

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

vpn load-balancing コマンドを使用して、VPN ロードバランシング モードに入ります。次のコマンドは、VPN ロードバランシング モードで使用できます。

cluster encryption

cluster ip address

cluster key

cluster port

interface

nat

participate

priority

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

次に **vpn load-balancing** コマンドの例を示します。プロンプト内の変化に注意してください。

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

次に、クラスタのパブリック インターフェイスを「test」として、クラスタのプライベート インターフェイスを「foo」として指定するインターフェイス コマンドを含む、VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロードバランシング実行時のコンフィギュレーションを削除して、ロードバランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロードバランシング実行時の統計情報を表示します。

vpn-sessiondb logoff

すべての VPN セッションまたは選択した VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff {**remote | l2l | webvpn | email-proxy | protocol** *protocol-name* | **name** *username* | **ipaddress** *IPaddr* | **tunnel-group** *groupname* | **index** *indexnumber* | **all**}

シンタックスの説明

all	すべての VPN セッションをログオフします。
email-proxy	すべての電子メール プロキシ セッションをログオフします。
index *indexnumber*	インデックス番号ごとにシングル セッションをログオフします。セッションのインデックス番号を指定します。
ipaddress *IPaddr*	指定した IP アドレスのセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザ名のセッションをログオフします。
protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルには、次の種類があります。 IKE　POP3S IMAP4S　SMTPS IPSec　userHTTPS IPSecLAN2LAN　vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	すべてのリモートアクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネルグループのセッションをログオフします。
webvpn	すべての WebVPN セッションをログオフします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

例

次の例では、すべてのリモートアクセス セッションをログオフする方法を示します。

```
hostname# vpn-sessiondb logoff remote
```

次の例では、すべての IPSec セッションをログオフする方法を示します。

```
hostname# vpn-sessiondb logoff protocol IPSec
```

vpn-sessiondb max-session-limit

VPN セッションをセキュリティ アプライアンスが許可しているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-session-limit** コマンドを使用します。セッションの制限値を削除するには、このコマンドの **no** 形式を使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-session-limit {*session-limit*}

no **vpn-sessiondb max-session-limit**

シンタックスの説明

session-limit	許容する VPN セッションの最大数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドは WebVPN を含むすべてのタイプの VPN セッションに適用されます。

例

次の例では、VPN セッションの最大制限値である 450 に設定する方法を示します。

```
hostname# vpn-sessiondb max-session-limit 450
```

vpn-session-timeout

VPN 接続に許可される最大時間を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、タイムアウト値を別のグループポリシーから継承できます。値を継承しないようにするには、**vpn-session-timeout none** コマンドを使用します。

vpn-session-timeout {*minutes* | **none**}

no vpn-session-timeout

シンタックスの説明

minutes	タイムアウト期間を分単位で指定します。1 ～ 35,791,394 の整数を使用します。
none	無制限のセッション タイムアウト期間を許容します。セッション タイムアウトにヌル値を設定して、セッション タイムアウトを拒否します。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

例

次の例では、FirstGroup という名前のグループポリシーに対して 180 分の VPN セッション タイムアウトを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

関連コマンド

group-policy	グループポリシーを作成または編集します。
vpn-idle-timeout	ユーザ タイムアウト期間を設定します。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

vpn-simultaneous-logins

ユーザに許容される同時ログイン数を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループポリシーから継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

シンタックスの説明

integer	0 ～ 2147483647 の数値です。

デフォルト

デフォルトの同時ログイン数は 3 です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

例

次の例では、FirstGroup という名前のグループポリシーに対して最大 4 つの同時ログインを許可する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN トンネル タイプ（IPSec または WebVPN）を設定するには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-tunnel-protocol** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpn-tunnel-protocol {webvpn | IPSec}

no vpn-tunnel-protocol [webvpn | IPSec]

シンタックスの説明

IPSec	2 つのピア間（リモートアクセス クライアントまたはその他のセキュアなゲートウェイ）で IPSec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を管理するセキュリティ結合を作成します。
webvpn	HTTPS 対応の Web ブラウザを経由してリモート ユーザに VPN サービスを提供します。クライアントは不要です。

デフォルト

IPSec です。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して 1 つ以上のトンネリング モードを設定します。VPN トンネルを越えて接続するには、ユーザに対して少なくとも 1 つのトンネリング モードを設定する必要があります。

例

次の例では、「FirstGroup」という名前のグループポリシーに対して WebVPN および IPSec トンネリング モードを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol webvpn
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

webvpn

グローバル コンフィギュレーション モードで WebVPN モードに入るには、**webvpn** コマンドを入力します。このコマンドと一緒に入力したコマンドを削除するには、**no webvpn** コマンドを使用します。これらの webvpn コマンドはすべての WebVPN ユーザに適用されます。

これらの webvpn コマンドを使用すると、エンド ユーザに表示される WebVPN 画面だけでなく、AAA サーバ、デフォルトのグループポリシー、デフォルトのアイドル タイムアウト、http プロキシおよび https プロキシ、NBNS サーバを、WebVPN に対して設定できるようになります。

webvpn

no webvpn

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

WebVPN は、デフォルトではディセーブルになっています。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

この WebVPN モードを使用すると、WebVPN のグローバル設定値を設定できます。グループポリシー モードまたはユーザ名モードのいずれかから入って WebVPN モードを使用すると、特定のユーザポリシーまたはグループポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

例

次の例では、WebVPN コマンド モードに入る方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)#
```

webvpn (group-policy, username)

この WebVPN モードに入るには、グループポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用します。WebVPN モードで入力したコマンド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。これらの webvpn コマンドは、設定するユーザ名またはグループポリシーに適用されます。

グループポリシーおよびユーザ名に対する webvpn コマンドにより、WebVPN を超えたファイル、MAPI プロキシ、URL および TCP アプリケーションへのアクセスが定義されます。また、ACL およびフィルタリングするトラフィックのタイプも識別されます。

webvpn

no webvpn

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

WebVPN は、デフォルトではディセーブルになっています。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードから入って WebVPN モードを使用すると、WebVPN のグローバル設定値を設定できます。

この項で説明したように、グループポリシー モードまたはユーザ名モードから入って WebVPN モードを使用すると、特定のユーザポリシーまたはグループポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

電子メール プロキシを使用するために WebVPN を設定する必要はありません。

WebVPN を使用すると、セキュリティ アプライアンスに対して Web ブラウザを使用したセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェア クライアントもハードウェア クライアントも必要ありません。WebVPN は、インターネット上のほとんどすべてのコンピュータから、広範囲の Web リソースおよび Web 対応アプリケーションに簡単にアクセスできる機能を提供します。WebVPN は SSL およびその後継である TLS1 を使用して、リモート ユーザとホスト側で設定した特定のサポートされる内部リソースとの間でセキュアな接続を提供します。セキュリティ アプライアンスはプロキシする必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

例

次の例では、FirstGroup という名前のグループポリシーに対して WebVPN モードに入る方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
filter	WebVPN 接続で使用するアクセスリストを指定します。
functions	ファイル アクセスとファイル ブラウジング、MAPI プロキシ、および WebVPN を超える URL エントリを設定します。
homepage	WebVPN ユーザがログインしたときに表示する Web ページの URL を設定します。
html-content-filter	WebVPN セッションに対してフィルタリングする Java、ActiveX、イメージ、スクリプト、およびクッキーを指定します。
port-forward	WebVPN アプリケーション アクセスをイネーブルにします。
port-forward-name	エンド ユーザに転送する TCP ポートを識別する表示名を設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバおよび URL のリストを指定します。

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するには、特権 EXEC モードで **who** コマンドを使用します。

who [*local_ip*]

シンタックスの説明

local_ip	（オプション）リストを 1 つの内部 IP アドレスまたはネットワーク アドレス（IPv4 または IPv6）に制限するために指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

who コマンドを使用すると、現在セキュリティ アプライアンスにログインしている各 Telnet クライアントの TTY_ID および IP アドレスを表示できます。

例

次の例では、クライアントが Telnet セッションを通してセキュリティ アプライアンスにログインした場合の ***who*** コマンドの出力を示します。

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
telnet	Telnet アクセスをセキュリティ アプライアンス コンソールに追加し、アイドル タイムアウトを設定します。

window-variation

さまざまなウィンドウ サイズの接続をドロップするには、tcp マップ コンフィギュレーション モードで **window-variation** 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。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

シンタックスの説明

allow-connection	接続を許可します。
drop-connection	接続をドロップします。

デフォルト

デフォルト アクションは、接続を許可します。

コマンドのモード

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
7.0	このコマンドが導入されました。

使用上のガイドライン

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ともに使用します。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 **window-variation** コマンドを使用して、縮小されたウィンドウ サイズの接続をすべてドロップします。

ウィンドウ サイズ メカニズムを使用すると、TCP は大きなウィンドウをアドバタイズした後、多すぎるデータを受信することなく、小さなウィンドウにアドバタイズできます。TCP の仕様では、「ウィンドウの縮小」は推奨されていません。この状態が検出されると、接続をドロップできます。

例

次の例では、さまざまなウィンドウ サイズの接続をすべて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)# window-variation drop-connection
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。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
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。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループポリシー コンフィギュレーション モードで **wins-server** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、WINS サーバを別のグループポリシーから継承できます。サーバを継承しないようにするには、**wins-server none** コマンドを使用します。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

シンタックスの説明

none	WINS サーバにヌル値を設定して、WINS サーバを許可しないようにします。デフォルトのグループポリシーまたは指定されているグループポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更
7.0	このコマンドが導入されました。

使用上のガイドライン

wins-server コマンドを発行するたびに、既存の設定を上書きします。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番目のコマンドが最初のコマンドを上書きします。したがって、y.y.y.y は唯一の WINS サーバになります。サーバを複数設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときにすべての WINS サーバの IP アドレスを含めます。

例

次の例では、FirstGroup という名前のグループポリシーに対して IP アドレス 10.10.10.15、10.10.10.30、および 10.10.10.45 で WINS サーバを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションはそのまま残ります。

write erase

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、セキュリティ コンテキスト内ではサポートされません。コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドにより識別されます。コンテキスト コンフィギュレーションを削除する場合は、リモート サーバ（指定されている場合）からファイルを手作業で削除するか、システム実行スペースで **delete** コマンドを使用してフラッシュ メモリからファイルを消去します。

例

次の例では、スタートアップ コンフィギュレーションを消去します。

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
delete	フラッシュ メモリからファイルを削除します。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

write memory

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

実行コンフィギュレーションは、メモリ内で現在実行されているコンフィギュレーションです。コマンドラインで行った変更がすべて含まれています。変更をスタートアップ コンフィギュレーションに保存する場合は、リブートの間だけ保存されます。これは起動時に実行中のメモリにロードされるコンフィギュレーションです。シングル コンテキスト モード、およびマルチ コンテキスト モードのシステムに対するスタートアップ コンフィギュレーションの場所は、デフォルトの場所（隠しファイル）から **boot config** コマンドを使用して選択した場所に変更できます。マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定した場所にあります。

マルチ コンテキスト モードでこのコマンドを実行すると、現在のコンフィギュレーションのみ保存されます。1 回のコマンドですべてのコンテキストを保存することはできません。システムおよび各コンテキストについて、このコマンドを個別に入力する必要があります。コンテキストのスタートアップ コンフィギュレーションは外部サーバ上に配置できます。この場合、セキュリティ アプライアンスは、コンフィギュレーションをサーバに戻して保存することができない HTTP および HTTPS URL を除き、**config-url** コマンドで指定したサーバにコンフィギュレーションを戻して保存します。システムは管理コンテキスト インターフェイスを使用して、コンテキストのスタートアップ コンフィギュレーションにアクセスするため、**write memory** コマンドも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。

write memory コマンドは、**copy running-config startup-config** コマンドと同じです。

例

次の例では、スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存します。

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
boot	ブート イメージおよびスタートアップ コンフィギュレーションを設定します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

write net

TFTP サーバに実行コンフィギュレーションを保存するには、特権 EXEC モードで **write net** コマンドを使用します。

write net [*server:*[*filename*] | *:filename*]

シンタックスの説明

:filename	パスとファイル名を指定します。**tftp-server** コマンドを使用してファイル名をすでに設定している場合、この引数はオプションです。 **tftp-server** コマンドで名前を指定したように、このコマンドでファイル名を指定すると、セキュリティ アプライアンスは **tftp-server** コマンド ファイル名をディレクトリとして扱い、***write net*** コマンド ファイル名をディレクトリの下のファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。TFTP サーバがこのタイプの URL をサポートしていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。このアドレスが存在する場合は、**tftp-server** コマンドで設定したアドレスを上書きします。 デフォルト ゲートウェイ インターフェイスは最高レベルのセキュリティ インターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

実行コンフィギュレーションは、メモリ内で現在実行されているコンフィギュレーションです。コマンドラインで行った変更がすべて含まれています。

マルチ コンテキスト モードでこのコマンドを実行すると、現在のコンフィギュレーションのみ保存されます。1 回のコマンドですべてのコンテキストを保存することはできません。システムおよび各コンテキストについて、このコマンドを個別に入力する必要があります。**write net** コマンドは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。ただし、システムは管理コンテキスト インターフェイスを使用して、コンテキストのスタートアップ コンフィギュレーションにアクセスするため、**write memory** コマンドは管理コンテキスト インターフェイスを使用して、スタートアップ コンフィギュレーションに保存します。

write net コマンドは、**copy running-config tftp** コマンドと同じです。

例

次の例では、**tftp-server** コマンドに TFTP サーバとファイル名を設定しています。

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

次の例では、**write net** コマンドにサーバとファイル名を設定しています。**tftp-server** コマンドは入力されません。

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

次の例では、**write net** コマンドにサーバとファイル名を設定しています。**tftp-server** コマンドはディレクトリ名を示し、サーバ アドレスは上書きされます。

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
copy running-config tftp	実行コンフィギュレーションを TFTP サーバにコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write standby

フェールオーバー スタンバイ装置にセキュリティ アプライアンスまたはコンテキストの実行コンフィギュレーションをコピーするには、特権 EXEC モードで **write standby** コマンドを使用します。

write standby

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
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

Active/Standby フェールオーバーの場合、**write standby** コマンドは、アクティブなフェールオーバー装置の RAM に保存されているコンフィギュレーションを、スタンバイ装置の RAM に書き込みます。プライマリ装置とセカンダリ装置のコンフィギュレーションの情報が異なる場合は、**write standby** コマンドを使用します。このコマンドをアクティブ装置に入力します。

Active/Active フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力すると、システム コンフィギュレーションおよびセキュリティ アプライアンス上のセキュリティ コンテキストのすべてのコンフィギュレーションはピア装置に書き込まれます。これは、スタンバイ状態にあるセキュリティ コンテキストのコンフィギュレーション情報を含みます。アクティブ状態のフェールオーバー グループ 1 を持つ装置のシステム実行スペースに、このコマンドを入力する必要があります。
- セキュリティ コンテキストに **write standby** コマンドを入力する場合、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストに、このコマンドを入力する必要があります。

（注）　**write standby** コマンドはコンフィギュレーションをピア装置の実行コンフィギュレーションに複製します。コンフィギュレーションはスタートアップ コンフィギュレーションには保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドを入力したのと同じ装置で **copy running-config startup-config** コマンドを使用します。コマンドはピア装置に複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

例

次の例では、現在の実行コンフィギュレーションをスタンバイ装置に書き込みます。

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ装置を強制的にリブートします。

write terminal

端末に実行コンフィギュレーションを表示するには、特権 EXEC モードで **write terminal** コマンドを使用します。

write terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンドのモード

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
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同じです。

例

次の例では、端末に実行コンフィギュレーションを書き込みます。

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。