CHAPTER 32

telnet ～ tunnel-limit コマンド

telnet

コンソールに Telnet アクセスを追加し、アイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet** コマンドを使用します。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	FWSM 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 接続先のネットワーク インターフェイスの名前を指定します。
IP_address	FWSM へのログインが許可されているホストまたはネットワークの IP アドレスを指定します。
IPv6_address	FWSM へのログインが許可されている IPv6 アドレス / プレフィクスを指定します。
mask	IP アドレスに対応付けられたネットマスクを指定します。
timeout *number*	FWSM によって終了されるまでの Telnet セッションのアイドル期間（分）を指定します。有効値は 1 ～ 1440 分です。

デフォルト

デフォルトでは、アイドル時間が 5 分に達すると Telnet セッションは FWSM により終了されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	変数 *IPv6_address* が追加されました。**no telnet timeout** コマンドが追加されました。

使用上のガイドライン

telnet コマンドを使用すると、FWSM コンソールに Telnet でアクセスできるホストを指定できます。すべてのインターフェイス上で FWSM への Telnet 接続をイネーブルにできます。ただし、FWSM は外部インターフェイスへのすべての Telnet トラフィックを IPSec で保護します。外部インターフェイスへの Telnet セッションをイネーブルにするには、FWSM で生成される IP トラフィックを追加するように外部インターフェイス上の IPSec を設定し、外部インターフェイス上で Telnet をイネーブルにします。

設定済みの IP アドレスからの Telnet アクセスを削除するには、**no telnet** コマンドを使用します。FWSM によってログオフされるまでのコンソール Telnet セッションの最大アイドル期間を設定するには、**telnet timeout** コマンドを使用します。**no telnet** コマンドと **telnet timeout** コマンドは併用できません。

IP アドレスを入力する場合は、ネットマスクも入力する必要があります。デフォルトのネットマスクはありません。内部ネットワークのサブネット マスクは使用しないでください。*netmask* は IP アドレスのビット マスクにすぎません。アクセスを単一の IP アドレスに制限するには、各オクテットに 255 を指定します（255.255.255.255 など）。

IPSec が動作している場合は、非セキュアなインターフェイス名（通常は外部インターフェイス）を指定できます。最低でも、**telnet** コマンドを使用してインターフェイス名を指定するように、**crypto map** コマンドを設定してください。

コンソールへの Telnet アクセス用パスワードを設定するには、**passwd** コマンドを使用します。デフォルトは **cisco** です。FWSM コンソールに現在アクセスしている IP アドレスを表示するには、**who** コマンドを使用します。アクティブな Telnet コンソール セッションを終了するには、**kill** コマンドを使用します。

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

（注） FWSM Telnet コンソール アクセスおよびコンソール ログイン要求タイムアウトに対して認証が必要となるように、**aaa** コマンドを設定した場合は、FWSM ユーザ名および **enable password** コマンドによって設定されたパスワードを入力して、シリアル コンソールから FWSM にアクセスできます。

例

次に、ホスト 192.168.1.3 および 192.168.1.4 が Telnet を介して FWSM コンソールにアクセスできるように設定する例を示します。192.168.2.0 ネットワーク上のすべてのホストにもアクセスが許可されます。

```
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
```

次に、最大セッション アイドル期間を変更する例を示します。

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

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

```
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エントリを個別に削除したり、**clear configure telnet** コマンドを使用して telnet コマンド ステートメントをすべて削除することができます。

```
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	FWSM への Telnet 接続に使用できる現在の IP アドレス リストを表示します。
who	FWSM 上でアクティブな Telnet 管理セッションを表示します。

terminal

現在の Telnet セッション中にシステム ログ メッセージを表示できるようにするには、特権 EXEC モードで **terminal monitor** コマンドを使用します。システム ログ メッセージをディセーブルにするには、**terminal no monitor** コマンドを使用します。

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

シンタックスの説明

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

デフォルト

デフォルトでは、システム ログ メッセージはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

例

次に、現在の Telnet セッションに対してのみロギングをイネーブルにして、そのあとディセーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
pager	Telnet セッション中に [---more---] プロンプトの前に表示される行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal pager	Telnet セッション中に [---more---] プロンプトの前に表示される行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードで端末表示幅を設定します。

terminal pager

Telnet セッション中に [---more---] プロンプトの前に表示される 1 ページあたりの行数を設定するには、特権 EXEC モードで **terminal pager** コマンドを使用します。

terminal pager [lines] *lines*

シンタックスの説明

[**lines**] *lines*	[---more---] プロンプトの前に表示される 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 を指定するとページ制限はなくなります。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは省略できます。指定しても、しなくても、コマンドは同じです。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが ***pager*** コマンドから変更されました。**pager** コマンドは現在、グローバル コンフィギュレーション モード コマンドです。

使用上のガイドライン

このコマンドは、現在の Telnet セッションにかぎって、ページャの行設定を変更します。新しいデフォルト ページャ設定をコンフィギュレーションに保存するには、**pager** コマンドを使用します。

管理コンテキストに、またはシステム実行スペースに対するセッションに Telnet 接続している場合に、別のコンテキストに切り替えると、所定のコンテキストにおける **pager** コマンドの設定に関係なく、ページャの行設定はユーザ セッションの設定に従います。現在のページャ設定を変更するには、新しい設定値を指定して **terminal pager** コマンドを入力するか、現在のコンテキストで **pager** コマンドを入力します。**pager** コマンドを使用すると、コンテキストのコンフィギュレーションに新しいページャ設定が保存されるだけでなく、現在の Telnet セッションにも新しい設定が適用されます。

例

次に、表示行数を 20 に変更する例を示します。

```
hostname# terminal pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
pager	Telnet セッション中に [---more---] プロンプトの前に表示される行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal	Telnet セッションでシステム ログ メッセージを表示できるようにします。
terminal width	グローバル コンフィギュレーション モードで端末表示幅を設定します。

terminal width

コンソール セッション中の情報表示幅を設定するには、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。この設定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。

terminal *width* *columns*

no terminal *width* *columns*

シンタックスの説明

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

デフォルト

デフォルト表示幅は 80 カラムです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

例

次に、端末の表示幅を 100 カラムに設定する例を示します。

```
hostname# terminal width 100
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
show running-config terminal	現在の端末設定を表示します。
terminal	特権 EXEC モードで端末行パラメータを設定します。

tftp-server

configure net または **write net** コマンドで使用するデフォルトの TFTP（簡易ファイル転送プロトコル）サーバおよびパスとファイル名を指定するには、グローバル コンフィギュレーション モードで **tftp-server** コマンドを使用します。サーバ設定を削除するには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 アドレスをサポートします。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

シンタックスの説明

interface_name	ゲートウェイ インターフェイスの名前を指定します。セキュリティが最大でないインターフェイスを指定すると、インターフェイスがセキュアでないことを示す警告メッセージが表示されます。
server	TFTP サーバの IP アドレスまたは名前を設定します。IPv4 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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	ゲートウェイ インターフェイスが必要になりました。

使用上のガイドライン

tftp-server コマンドを使用すると、**configure net** および **write net** コマンドを簡単に入力できるようになります。**configure net** または **write net** コマンドを入力する場合は、**tftp-server** コマンドで指定された TFTP サーバを継承したり、独自に値を指定することができます。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および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。

FWSM がサポートする **tftp-server** コマンドは 1 つのみです。

例

次に、TFTP サーバを指定して、/temp/config/test_config ディレクトリからコンフィギュレーションを読み取る例を示します。

```
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 アドレスおよび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

最大アイドル時間を設定するには、グローバル コンフィギュレーション モードで **timeout** コマンドを使用します。

timeout {**xlate** | **conn** | **half-closed** | **udp** | **icmp** | **h225** | **h323** | **mgcp** | ***mgcp-pat*** | **sip** | **sip_media** | **non_tcp_udp** | **sunrpc** | **uauth**} *hh*:*mm*:*ss*

シンタックスの説明

conn	接続が終了するまでのアイドル時間を指定します。最小値は 5 分です。
hh:*mm*:*ss*	タイムアウトを指定します。
h225	H.225 シグナリング接続が終了するまでのアイドル時間を指定します。
h323	H.245（TCP）および H.323（UDP）メディア接続が終了するまでのアイドル時間を指定します。デフォルトは 5 分です。 （注）　H.245 と H.323 のメディア接続には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 タイムアウトが同じになります。
half-closed	半分終了した TCP 接続が解放されるまでのアイドル時間を指定します。
icmp	ICMP のアイドル時間を指定します。
mgcp	MGCP メディア接続が削除されるまでのアイドル時間を設定します。
mgcp-pat	MGCP PAT 変換が削除されるまでの絶対的なインターバルを設定します。
non_tcp_udp	TCP/UDP 以外の接続が終了するまでのアイドル時間を設定します。
sip	SIP タイマーを変更します。
sip_media	UDP 非アクティビティ タイムアウトでなく、SIP UDP メディア パケットによる SIP RTP/RTCP に使用される SIP メディア タイマーを変更します。
sunrpc	SUNRPC スロットが終了するまでのアイドル時間を指定します。
uauth	認証および許可キャッシュがタイムアウトし、ユーザが次の接続を再認証するまでの期間を設定します。
udp	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。最小値は 1 分です。
xlate	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。最小値は 1 分です。

デフォルト

デフォルトの設定は次のとおりです。

- **conn** *hh*:*mm*:*ss* — 1 時間（**01:00:00**）
- **h255** *hh*:*mm*:*ss* — 1 時間（**01:00:00**）
- **h323** *hh*:*mm*:*ss* — 5 分（**00:05:00**）
- **half-closed** *hh*:*mm*:*ss* — 10 分（**00:10:00**）
- **icmp** *hh:mm:ss* — 2 分（**00:00:02**）
- **mgcp** *hh:mm:ss* — 5 分（**00:05:00**）
- **mgcp-pat** *hh:mm:ss* — 5 分（**00:05:00**）
- **non_tcp_udp** *hh:mm:ss* — 10 分（**00:10:00**）
- **sip** *hh:mm:* — 30 分（**00:30:00**）
- **sip_media** *hh:mm:ss* — 2 分（**00:02:00**）
- **sunrpc** *hh:mm:ss* — 10 分（**00:10:00**）

- **uauth** タイマー **— absolute**
- **udp** *hh*:*mm*:*ss* **—** 2 分（**00:02:00**）
- **xlate** *hh*:*mm*:*ss* **—** 3 時間（**03:00:00**）

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。
3.1(1)	キーワード ***mgcp-pat*** が追加されました。**rpc** キーワードが **sunrpc** に変更されました。

使用上のガイドライン

timeout コマンドを使用すると、複数のプロセスのアイドル時間を設定できます。指定したアイドル時間の間スロットが使用されなかった場合、リソースは空いているプールに戻されます。通常の接続終了シーケンスのあと、TCP 接続スロットは約 60 秒間解放されます。

（注） 接続にパッシブ FTP（ファイル転送プロトコル）が使用されている場合、または Web 認証に **virtual** コマンドが使用されている場合は、**timeout uauth 0:0:0** コマンドを使用しないでください。

接続タイマーは変換タイマーよりも優先します。変換タイマーが機能するのは、すべての接続がタイムアウトしたあとのみです。

conn *hh*:*mm*:*ss* を設定する場合に **0:0:0** を使用すると、接続がタイムアウトしなくなります。

half-closed *hh*:*mm*:*ss* を設定する場合に **0:0:0** を使用すると、半分終了した接続がタイムアウトしなくなります。

h255 *hh*:*mm*:*ss* を設定する場合に **h225 00:00:00** を設定すると、H.225 シグナリング接続は切断されなくなります。タイマアウト値に **h225 00:00:01** を指定すると、タイマーはディセーブルになり、すべてのコールが削除された直後に TCP 接続が終了します。

uauth *hh*:*mm*:*ss* 期間は、**xlate** キーワードの値よりも小さくなければなりません。キャッシングをディセーブルにするには、**0** に設定します。接続上でパッシブ FTP を使用する場合は、ゼロに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 タイマーを **0**（ゼロ）に設定します。

例

次に、最大アイドル時間を設定する例を示します。

```
hostname(config)# timeout uauth 0:5:00 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	指定され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（認証、認可、アカウンティング）サーバとの接続確立を断念するまでの、ホスト固有の最大応答時間を設定するには、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、デフォルト値の 10 秒にタイムアウトをリセットするには、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	要求のタイムアウト間隔（1 ～ 60 秒）を指定します。この値は、FWSM がプライマリ AAA サーバへの要求を断念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、FWSM 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 モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

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 タイプに対して有効です。

FWSM が AAA サーバとの接続を試行する期間を指定するには、**timeout** コマンドを使用します。FWSM が接続を試行する間隔を指定するには、**retry-interval** コマンドを使用します。

タイムアウトは、FWSM がサーバとのトランザクションを実行しようとする合計時間です。再試行インターバルによって、タイムアウト期間中に通信を再試行する頻度が決まります。したがって、再試行インターバルがタイムアウト値以上であれば、再試行されません。再試行が必要な場合は、再試行インターバルをタイムアウト値よりも小さくする必要があります。

例

次に、タイムアウト値を 30 秒、再試行インターバルを 10 秒に、ホスト 1.2.3.4 の RADIUS AAA サーバ [svrgrp1] を設定する例を示します。FWSM は、30 秒後に断念するまでに通信を 3 回試行します。

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

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。GTP マップ コンフィギュレーション モードにアクセスするには、**gtp-map** コマンドを使用します。これらのインターバルをデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

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	タイムアウト値です。*hh* は時間、*mm* は分、*ss* は秒を指定します。値 0 を指定すると、すぐには切断されません。
gsn	GSN を削除するまでの非アクティビティ期間を指定します。
pdp-context	PDP コンテキストの受信を開始するまでの最大許容時間を指定します。
request	GTP メッセージの受信を開始するまでに最大許容時間を指定します。
signaling	GTP シグナリングを削除するまでの非アクティビティ期間を指定します。
tunnel	GTP トンネルを切断するまでの非アクティブ期間を指定します。

デフォルト

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

request のデフォルトは 1 分です。

tunnel のデフォルトは 1 分です（Delete PDP Context Request が受信されない場合）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

PDP コンテキストは、IMSI および NSAPI を組み合わせた TID で識別されます。各 MS には最大 15 の NSAPI を設定できるため、各 QoS（サービス品質）レベルのアプリケーション要件に基づいて、それぞれ異なる NSAPI を持つ複数の PDP コンテキストを作成することができます。

GTP トンネルは異なる GSN ノード内にある 2 つの対応する PDP コンテキストによって定義され、トンネル ID で識別されます。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 ユーザ間でパケットを転送する場合は、GTP トンネルが必要です。

例

次に、要求キューのタイムアウト値を 2 分に設定する例を示します。

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

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査の詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	特定の GTP マップがアプリケーション検査で使用されるようにします。
show service-policy inspect gtp	GTP 設定を表示します。

time-range

time-range コンフィギュレーション モードを開始し、トラフィック ルールまたはアクションに付加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。この設定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。

time-range *name*

no time-range *name*

シンタックスの説明

name	時間範囲の名前。名前の最大長は 64 文字です。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

時間範囲を作成しても、デバイスへのアクセスは制限されません。**time-range** コマンドは時間範囲のみを定義します。時間範囲を定義してから、トラフィック ルールまたはアクションに付加します。

時間ベースの ACL を実行するには、***time-range*** コマンドを使用して、特定の時刻と曜日を定義します。次に、**access-list extended time-range** コマンドを使用して時間範囲を ACL にバインドします。

時間範囲には FWSM のシステム クロックを使用しますが、機能が最適に動作するのは、NTP と同期した場合です。

例

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

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

時間範囲を作成し、time-range コンフィギュレーション モードを開始すると、**absolute** 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るようになります。***time-range*** コマンドの ***absolute*** および ***periodic*** キーワードをデフォルト設定にリセットするには、time-range 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。

時間ベースの ACL を実行するには、***time-range*** コマンドを使用して、特定の時刻と曜日を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドさせます。次に、ACL [Sales] を時間範囲 [New_York_Minute] にバインドさせる例を示します。

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

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

関連コマンド

コマンド	説明
absolute	時間範囲が有効となる絶対時刻を定義します。
access-list extended	FWSM を介して IP トラフィックを許可または拒否するポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** および ***periodic*** キーワードをデフォルト設定に戻します。
periodic	時間範囲機能をサポートする機能に、週単位の反復する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）をグループに収集してリフレッシュ、チェックサム、エージングを行うインターバルを指定するには、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 LSA をグループに収集して、リフレッシュ、チェックサム、またはエージングを行うインターバル。有効値は 10 ～ 1800 秒です。

デフォルト

デフォルトのインターバルは 240 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF LSA をグループに収集し、リフレッシュ、チェックサム、またはエージングを行うインターバルを変更するには、**timers lsa-group-pacing** *seconds* コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers lsa-group-pacing** コマンドを使用します。

例

次に、LSA のグループ処理インターバルを 500 秒に設定する例を示します。

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

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般的な情報を表示します。
timers spf	Shortest Path First（SPF）の計算遅延およびホールドタイムを指定します。

timers spf

Shortest Path First（SPF）計算の遅延およびホールドタイムを指定するには、ルータ コンフィギュレーション モードで **timers spf** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

シンタックスの説明

delay	OSPF がトポロジ変更を受信してから、SPF 計算を開始するまでの遅延時間を、1 ～ 65535 秒の範囲で指定します。
holdtime	連続する 2 つの SPF 計算間のホールドタイム（秒）。有効値は 1 ～ 65535 です。

デフォルト

デフォルトの設定は次のとおりです。

- *delay* ― 5 秒
- *holdtime* ― 10 秒

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

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

例

次に、SPF 計算の遅延を 10 秒、SPF 計算のホールドタイムを 20 秒に設定する例を示します。

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

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般的な情報を表示します。
timers lsa-group-pacing	OSPF LSA を収集して、リフレッシュ、チェックサム、またはエージングを行うインターバルを指定します。

transfer-encoding

転送符号化タイプを指定して、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。HTTP マップ コンフィギュレーション モードにアクセスするには、**http-map** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

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

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

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する接続が検出された場合に実行するアクションを指定します。
allow	メッセージを許可します。
chunked	メッセージ本体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	メッセージ本体が UNIX ファイル圧縮を使用して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にもかかわらず、コンフィギュレーション リストに存在しない要求方式がトラフィックに含まれている場合に、FWSM が実行するデフォルト アクションを指定します。
deflate	メッセージ本体が zlib 形式（RFC 1950）および deflate 圧縮（RFC 1951）を使用して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	メッセージ本体が GNU zip（RFC 1952）を使用して転送される転送符号化タイプを識別します。
identity	メッセージ本体が転送符号化を使用しないで転送される接続を識別します。
log	（任意）Syslog を生成します。
reset	クライアントおよびサーバに 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介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です。このコマンドがイネーブル化されていて、サポート対象の転送符号化タイプが指定されていない場合、デフォルトで接続は許可され、ロギングは行われません。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、別のデフォルト アクションを指定します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

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と、FWSM は設定されているサポート対象の転送符号化タイプごとに、指定されたアクションを HTTP 接続に適用します。

FWSM は **default** アクションを、設定リストの転送符号化タイプと*一致しない*すべてのトラフィックに適用します。設定済みの **default** アクションでは、ロギングを行わずに接続を**許可**します。

たとえば、設定済みのデフォルト アクションがある場合に、アクションが **drop** や **log** である符号化タイプを 1 つまたは複数指定すると、FWSM は設定済みの符号化タイプを含む接続を削除し、各接続をロギングし、その他のサポート対象符号化タイプに対応する接続をすべて許可します。

より限定的なポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log**（イベントを記録する場合）に変更します。次に、許可された符号化タイプごとに **allow** アクションを設定します。

適用する設定ごとに、**transfer-encoding** コマンドを 1 回入力します。デフォルト アクションを変更する場合、および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場合は、それぞれ別々の **transfer-encoding** コマンド インスタンスを使用します。

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 リストからアプリケーション カテゴリを削除した場合、コマンドライン内のそのアプリケーション カテゴリ キーワード後の文字列はすべて無視されます。

例

次に、設定済みのデフォルトを使用して、特に禁止されていないサポート対象アプリケーション タイプをすべて許可する、制限の緩いポリシーを設定する例を示します。

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

この場合、GNU zip を使用する接続のみが削除され、イベントが記録されます。

次に、接続をリセットし、特に許可されていないすべての符号化タイプに対応するイベントを記録するようにデフォルト アクションを変更して、限定的なポリシーを設定する例を示します。

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

この場合、転送符号化を使用しない接続のみが許可されます。サポート対象のその他の符号化タイプに対応した HTTP トラフィックが受信されると、FWSM は接続をリセットし、Syslog エントリを作成します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張 HTTP 検査に関連付けられたトラフィックの詳細情報を表示します。
http-map	拡張 HTTP 検査を設定するために HTTP マップを定義します。
inspect http	特定の HTTP マップがアプリケーション検査で使用されるようにします。
policy-map	特定のセキュリティ アクションにクラス マップを対応付けます。

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、tunnel-group ipsec-attributes モードで **trust-point** コマンドを使用します。トラストポイントの指定を除去するするには、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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
tunnel-group ipsec-attributes コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

すべてのトンネルグループ タイプにこの属性を適用できます。

例

次に、config-ipsec コンフィギュレーション モードでコマンドを入力し、IPSec LAN-to-LAN トンネル グループ 209.165.200.225 の IKE ピアに送信する証明書を識別するためのトラストポイントを設定する例を示します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル グループをすべて消去します。
crypto ca trustpoint	指定したトランスポートでトラストポイント モードを開始します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの設定を表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。

tunnel-group

IPSec の接続固有レコードのデータベースを作成および管理するには、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 グループ名を指定します。任意の文字列を選択できます。名前に IP アドレスを指定する場合は、通常、ピアの IP アドレスを使用します。
type	トンネル グループのタイプを指定します。 L2TP/IPSec — L2TP over IPSec ipsec-ra — IPSec リモート アクセス ipsec-l2l — IPsec LAN-to-LAN

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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 コマンドをトランスペアレント ファイウォール モードで使用すると、LAN-to-LAN トンネル グループを設定できますが、リモートアクセス グループを設定することはできません。LAN-to-LAN で使用できるすべての tunnel-group コマンドは、トランスペアレント ファイウォール モードでも使用できます。

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM にはデフォルト トンネル グループが 2 つあります。IPSec リモートアクセス トンネル グループのデフォルトである DefaultRAGroup と、IPSec LAN-to-LAN トンネル グループのデフォルトである DefaultL2Lgroup です。これらのデフォルト トンネル グループは変更できますが、削除することはできません。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かった場合、FWSM はこれらのグループを使用して、リモート アクセスおよび LAN-to-LAN トンネル グループのデフォルト トンネル パラメータを設定します。

tunnel-group コマンドには、次のコマンドがあります。これらの各コマンドを実行するとコンフィギュレーション モードが開始し、コンフィギュレーション モードのレベルで属性を設定できるようになります。

- **tunnel-group general-attributes**

- **tunnel-group ipsec-attributes**
- **tunnel-group ppp-attributes**

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、IPSec LAN-to-LAN トンネル グループを設定する例を示します。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	設定されたトンネル グループをすべて消去します。
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 グループ設定を表示します。
tunnel-group map	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。

tunnel-group general-attributes

general-attributes コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **tunnel-group general-attributes** コマンドを使用します。このモードは、サポートされているすべてのトンネリング プロトコルに共通の設定値を設定する場合に使用します。

一般属性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属性を指定します。
name	トンネル グループ名を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

次の表に、このグループに属するコマンド、およびこれらのコマンドを設定できるトンネルグループ タイプを示します。

一般属性	使用可能なトンネルグループ タイプ
accounting-server-group	IPSec RA、IPSec L2L、L2TP/IPSec
address-pool	IPSec RA、L2TP/IPSec
authentication-server-group	IPSec RA、L2TP/IPSec
authorization-server-group	IPSec RA、L2TP/IPSec
default-group-policy	IPSec RA、IPSec L2L、L2TP/IPSec
dhcp-server	IPSec RA、L2TP/IPSec
strip-group	IPSec RA、L2TP/IPSec
strip-realm	IPSec RA、L2TP/IPSec

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、LAN-to-LAN ピアの IP アドレスを使用して IPSec LAN-to-LAN 接続のトンネル グループを作成し、一般属性を設定するための一般コンフィギュレーション モードを開始する例を示します。トンネル グループ名は 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)#
```

次に、グローバル コンフィギュレーション モードでコマンドを入力し、IPSec リモート アクセス接続のトンネル グループ [remotegrp] を作成し、トンネル グループ [remotegrp] の一般属性を設定するための一般コンフィギュレーション モードを開始する例を示します。

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

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたトンネル グループをすべて消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの設定を表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリにトンネル グループを対応付けます。

tunnel-group ipsec-attributes

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

IPSec 属性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属性を指定します。
name	トンネル グループ名を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

このグループに属するコマンドは、次のとおりです。

IPSec 属性	使用可能なトンネルグループ タイプ
authorization-dn-attributes	IPSec RA
authorization-required	IPSec RA
chain	IPSec RA、IPSec L2L、L2TP/IPSec
client-update	IPSec RA
isakmp keepalive	IPSec RA
peer-id-validate	IPSec RA、IPSec L2L、L2TP/IPSec
pre-shared-key	IPSec RA、IPSec L2L、L2TP/IPSec
radius-with-expiry	IPSec RA
trust-point	IPSec RA、IPSec L2L、L2TP/IPSec

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、IPSec リモートアクセス トンネル グループ [remotegrp] のトンネル グループを作成し、IPSec グループ属性を指定する例を示します。

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

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name（crypto ca certificate map）	ルール エントリの文字列と比較する CA 証明書の DN を識別します。
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-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 グループにマッピングする場合に使用するポリシーおよびルールを設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに対応付けるには、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 インデックスを複数回参照しないかぎり、このコマンドは何度でも呼び出すことができます。

トンネルグループマップを削除するには、このコマンドの **no** 形式を使用します。

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

no tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

シンタックスの説明

default-group *tunnel-group-name*	設定されているその他の方式で名前を取得できない場合に使用する、デフォルト トンネル グループを指定します。*tunnel-group name* は常に存在している必要があります。
rule index	（任意）**crypto ca certificate map** コマンドで指定されたパラメータを参照します。指定できる値は 1 ～ 65535 です。

デフォルト

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

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

crypto ca certificate map コマンドは、プライオリティが設定された証明書マッピング ルール リストをメンテナンスします。存在できるマップは 1 つのみですが、このマップには最大 65535 のルールを含めることができます。詳細については、**crypto ca certificate map** コマンドの説明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では、トンネル グループに対応付けられていない証明書マップ内のエントリ（このコマンドで識別されないすべてのマップ ルール）は無視されます。

例

次に、グローバル コンフィギュレーション モードでコマンドを入力し、設定されているその他の方式で名前を取得できない場合に使用する、デフォルト トンネル グループを指定する例を示します。使用するトンネル グループ名は 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	CA 証明書マップ モードを開始します。
subject-name（crypto ca certificate map）	ルール エントリの文字列と比較する CA 証明書の DN を識別します。

tunnel-group-map enable

証明書ベースの IKE セッションをトンネル グループにマッピングする場合に使用するポリシーおよびルールを設定するには、グローバル コンフィギュレーション モードで **tunnel-group-map enable** 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。

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

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

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ためのポリシーを指定します。*policy* には次のいずれかを指定できます。 **ike-id —** トンネルグループがルール検索に基づいて判別されない場合、または OU（組織単位）から取得されない場合に、証明書ベース IKE セッションが phase1 IKE ID の内容に基づいてトンネル グループにマッピングされるように指定します。 **ou —** トンネルグループがルール検索に基づいて判別されない場合に、サブジェクト DN（識別名）内の OU 値を使用するように指定します。 **peer-ip —** トンネルグループがルール検索に基づいて判別されない場合、または OU や IKE-ID 方式から取得されない場合に、確立されたピア IP アドレスを使用するように指定します。 **rules —** 証明書ベース IKE セッションが、このコマンドによって設定された証明書マップの対応付けに基づいてトンネル グループにマッピングされるように指定します。
rule index	（任意）**crypto ca certificate map** コマンドで指定されたパラメータを参照します。指定できる値は 1 ～ 65535 です。

デフォルト

tunnel-group-map コマンドのデフォルト値は DefaultRAGroup に設定されている **enable ou** および **default-group** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

crypto ca certificate map コマンドは、プライオリティが設定された証明書マッピング ルール リストをメンテナンスします。存在できるマップは 1 つのみですが、このマップには最大 65535 のルールを含めることができます。詳細については、**crypto ca certificate map** コマンドの説明を参照してください。

例

次に、phase1 IKE ID の内容に基づいて、トンネル グループに証明書ベース IKE セッションのマッピングをイネーブルにする例を示します。

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

次に、確立されたピア 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 IKE セッションのマッピングをイネーブルにする例を示します。

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

次に、サブジェクト DN 内の OU に基づいて、証明書ベース IKE セッションのマッピングをイネーブルにする例を示します。

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

次に、確立されたルールに基づいて、証明書ベース IKE セッションのマッピングをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードを開始します。
subject-name（crypto ca certificate map）	ルール エントリの文字列と比較する CA 証明書の DN を識別します。

tunnel-limit

FWSM でアクティブにできる 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。GTP マップ コンフィギュレーション モードにアクセスするには、**gtp-map** コマンドを使用します。トンネル制限をデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

シンタックスの説明

max_tunnels	許容される最大トンネル数です。指定できる範囲は 1 ～ 4294967295 です（トンネル全体の最大数）。

デフォルト

トンネル制限のデフォルトは 500 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	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
3.1(1)	このコマンドが追加されました。

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

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

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

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査の詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	特定の GTP マップがアプリケーション検査で使用されるようにします。
show service-policy inspect gtp	GTP 設定を表示します。