CHAPTER 31

shun ～ sysopt uauth allow-http-cache コマンド

shun

攻撃元ホストからの接続を遮断するには、特権 EXEC モードで **shun** コマンドを使用します。遮断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。

shun *src_ip* [*dst_ip src_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *src_ip* [**vlan** *vlan_id*]

シンタックスの説明

dest_port	（任意）遮断される接続の宛先ポートを指定します。
dst_ip	（任意）ターゲット ホストのアドレスを指定します。
protocol	（任意）UDP や TCP などの IP プロトコルを指定します。デフォルトのプロトコルは 0（任意のプロトコル）です。
src_ip	攻撃元ホストのアドレスを指定します。
src_port	（任意）遮断される接続の送信元ポートを指定します。
vlan_id	（任意）VLAN（仮想 LAN）ID を指定します。

デフォルト

デフォルトのプロトコルは 0（任意のプロトコル）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。

使用上のガイドライン

shun コマンドを使用すると、攻撃元ホストからの接続を遮断できます。ブロック機能が手動または Cisco IPS センサによって解除されないかぎり、コマンドに指定された値に一致するパケットは廃棄され、ログに記録され続けます。**shun** コマンドのブロック機能は、指定されたホスト アドレスによる接続が現在アクティブであるかどうかに関係なく適用されます。

宛先アドレス、送信元 / 宛先ポート、プロトコルをパラメータとして指定すると、それらのパラメータに一致する接続だけを遮断できます。

1 つの発信元 IP アドレスに関連付けることができる **shun** コマンドは 1 つだけです。

shun コマンドは攻撃を動的にブロックするために使用されるため、FWSM のコンフィギュレーションには表示されません。

インターフェイスを取り外すと、このインターフェイスに対応するすべての遮断機能も解除されます。新しいインターフェイスを追加するか、または（同名の）同じインターフェイスで置換した場合に、IPS センサでこのインターフェイスをモニタするには、IPS センサにこのインターフェイスを追加する必要があります。

例

次に、攻撃元ホスト（10.1.1.27）が攻撃対象（10.2.2.89）に TCP を使用して接続する例を示します。FWSM 接続テーブル内の接続は、次のようになります。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

次のオプションを使用して **shun** コマンドを適用します。

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

このコマンドを実行すると、FWSM 接続テーブルから該当する接続が削除され、10.1.1.27:555 から 10.2.2.89:666 への TCP パケットが FWSM を通過することもできなくなります。

関連コマンド

コマンド	説明
clear shun	現在イネーブル化されている遮断をすべてディセーブルにし、遮断に関する統計情報を消去します。
show conn	アクティブな接続をすべて表示します。
show shun	遮断情報を表示します。

shutdown

インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべての物理インターフェイスは、デフォルトでシャットダウンしています。セキュリティ コンテキスト内で割り当てられたインターフェイスは、コンフィギュレーション内でシャットダウンしません。

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
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
2.2(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

すべての物理インターフェイスは、デフォルトでシャットダウンしています。イネーブル化されたサブインターフェイスをトラフィックが通過する前に、物理インターフェイスをイネーブルにする必要があります。マルチ コンテキスト モードで、コンテキストに物理インターフェイスまたはサブインターフェイスを割り当てた場合、このコンテキスト内ではインターフェイスがデフォルトでイネーブルです。ただし、コンテキスト インターフェイスをトラフィックが通過する前に、システム コンフィギュレーションでもこのインターフェイスをイネーブルにする必要があります。システム実行スペースでインターフェイスをシャットダウンした場合、このインターフェイスは共有されるすべてのコンテキストでシャットダウンされます。

例

次に、サブインターフェイスをイネーブルにする例を示します。

```
hostname(config)# interface gigabitethernet2.1
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
```

次に、サブインターフェイスをシャットダウンする例を示します。

```
hostname(config)# interface gigabitethernet2.1
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)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存接続のすべての変換をリセットして、接続をリセットします。
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 モードを開始します。

sip-map

IP アドレス プライバシー機能をイネーブルにするために必要な SIP アプリケーション検査マップを識別するには、グローバル コンフィギュレーション モードで **sip-map** コマンドを使用します。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。

sip-map *map_name*

no sip-map *map_name*

シンタックスの説明

map_name	SIP マップの名前

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
FWSM 3.1	このコマンドが追加されました。

使用上のガイドライン

IP アドレス プライバシー機能をイネーブルにするために必要な SIP アプリケーション検査マップを識別するには、**sip-map** コマンドを使用します。このコマンドを入力すると、SIP マップ コンフィギュレーション モードが開始し、**ip-address-privacy** コマンドを入力できるようになります。SIP マップを定義したら、**inspect sip** コマンドを使用して、マップをイネーブルにします。次に、**class-map**、**policy-map**、および **service-policy** コマンドを使用して、トラフィック クラスを定義したり、このクラスに **inspect** コマンドを適用したり、1 つまたは複数のインターフェイスにポリシーを適用したりします。

例

次に、SIP トラフィックを識別し、SIP マップを定義し、ポリシーを定義して外部インターフェイスに適用する例を示します。

```
hostname(config)# access-list sip-acl permit tcp any any eq 5060
hostname(config)# class-map sip-port
hostname(config-cmap)# match access-list sip-acl
hostname(config-cmap)# sip-map inbound_sip
hostname(config-sip-map)# ip-address-privacy
hostname(config-sip-map)# policy-map S1_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip s1_policy
hostname(config)#
```

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。
ip-address-privacy	SIP アプリケーション検査の IP アドレス プライバシー機能をイネーブルにします。
inspect sip	SIP アプリケーション検査をイネーブルにします。
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。

smtp-server

SMTP 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 **smtp-server** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

FWSM には内部 SMTP クライアントが組み込まれています。イベント システムはこのクライアントを使用して、特定のイベントが発生したことを外部エンティティに通知できます。これらのイベント通知を受信し、指定された電子メール アドレスに転送するように SMTP サーバを設定できます。SMTP 機能がアクティブになるのは、FWSM で電子メール イベントがイネーブルな場合のみです。

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

シンタックスの説明

primary_server	プライマリ SMTP サーバを識別します。IP アドレスまたは DNS 名を使用します。
backup_server	プライマリ SMTP サーバを使用できない場合にイベント メッセージをリレーするバックアップ SMTP サーバを識別します。IP アドレスまたは DNS 名を使用します。

デフォルト

デフォルトでは、SMTP サーバは設定されていません。

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)	このコマンドのサポートが追加されました。

使用上のガイドライン

例

次に、IP アドレスが 10.1.1.24 の SMTP サーバ、および IP アドレスが 10.1.1.34 のバックアップ SMTP サーバを設定する例を示します。

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp-map

SNMP（簡易ネットワーク管理プロトコル）検査用パラメータを定義するための特定のマップを識別するには、グローバル コンフィギュレーション モードで **snmp-map** コマンドを使用します。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。

snmp-map *map_name*

no snmp-map *map_name*

シンタックスの説明

map_name	SNMP マップの名前

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

SNMP 検査用パラメータを定義するための特定のマップを識別するには、**snmp-map** コマンドを使用します。このコマンドを入力すると、SNMP マップ コンフィギュレーション モードが開始し、特定のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップを定義したら、**inspect snmp** コマンドを使用して、マップをイネーブルにします。次に、**class-map**、**policy-map**、および **service-policy** コマンドを使用して、トラフィック クラスを定義したり、このクラスに **inspect** コマンドを適用したり、1 つまたは複数のインターフェイスにポリシーを適用したりします。

例

次に、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義して外部インターフェイスに適用する例を示します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

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。
deny version	特定のバージョンの SNMP を使用してトラフィックを禁止します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
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。

snmp-server community

SNMP（簡易ネットワーク管理プロトコル）コミュニティ ストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。コミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community *text*

no snmp-server community [*text*]

シンタックスの説明

text	コミュニティ ストリングを設定します。

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
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

SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象ネットワーク ノード間で共有されるシークレット ストリングです。FWSM はこの鍵を使用して、着信 SNMP 要求が有効かどうかを判別します。たとえば、コミュニティ ストリングを使用してサイトを指定してから、同じストリングを使用してルータ、FWSM、および管理ステーションを設定できます。FWSM はこのストリングを使用し、コミュニティ ストリングが無効な要求には応答しません。

例

次に、コミュニティ ストリングを wallawallabingbang に設定する例を示します。

```
hostname(config)# snmp-server community wallawallabingbang
```

関連コマンド

コマンド	説明
snmp-server contact	SNMP の担当者名を設定します。
snmp-server enable	FWSM で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバ ロケーション ストリングを設定します。

snmp-server contact

SNMP（簡易ネットワーク管理プロトコル）の担当者名を設定するには、グローバル コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。担当者名を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *text*

no snmp-server contact [*text*]

シンタックスの説明

text	担当者または FWSM システム管理者の名前を指定します。名前は大文字と小文字を区別する 127 文字以下の文字列です。スペースを含めることができますが、複数のスペースは 1 つのスペースに省略されます。

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
1.1(1)	このコマンドが追加されました。

例

次に、担当者を Pat Johnson に設定する例を示します。

```
hostname(config)# snmp-server contact Pat Johnson
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server enable	FWSM で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバ ロケーション ストリングを設定します。

snmp-server enable

FWSM で SNMP（簡易ネットワーク管理プロトコル）をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。SNMP 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。

snmp-server enable

no snmp-server enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトで、SNMP サーバはイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このコマンドを使用すると、SNMP トラップやその他の設定を行ったり、これらを再設定しなくても、SNMP を簡単にイネーブルまたはディセーブルにすることができます。

例

次に、SNMP をイネーブルにし、SNMP ホストおよびトラップを設定し、トラップをシステム メッセージとして送信する例を示します。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の担当者名を設定します。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバ ロケーション ストリングを設定します。

snmp-server enable traps

FWSM から NMS へのトラップ送信をイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。トラップ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。

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

シンタックスの説明

all	すべてのトラップをイネーブルにします。
entity [*trap*]	エンティティ トラップをイネーブルにします。**entity** に指定できるトラップは、次のとおりです。 • **config-change** • **fru-insert** • **fru-remove**
ipsec [*trap*]	IPSec トラップをイネーブルにします。**ipsec** に指定できるトラップは、次のとおりです。 • **start** • **stop**
remote-access [*trap*]	リモート アクセス トラップをイネーブルにします。**remote-access** に指定できるトラップは、次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップをイネーブルにします。デフォルトでは、すべての SNMP トラップがイネーブルです。**snmp** に指定できるトラップは、次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	Syslog トラップをイネーブルにします。

デフォルト

デフォルト設定では、すべての **snmp** トラップがイネーブルです（**snmp-server enable traps snmp authentication linkup linkdown coldstart**）。これらのトラップをディセーブルにするには、このコマンドの **no** 形式に **snmp** キーワードを指定して使用します。ただし、**clear configure snmp-server** コマンドを使用すると、デフォルト設定に戻って SNMP トラップがイネーブルになります。

トラップ タイプを指定しないでこのコマンドを入力した場合は、デフォルトで **syslog** が適用されます（デフォルトの **snmp** トラップおよび **syslog** トラップは引き続きイネーブルです）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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。

使用上のガイドライン

個々のトラップまたは一連のトラップをイネーブルにする場合は、機能タイプごとにこのコマンドを入力します。すべてのトラップをイネーブルにする場合は、**all** キーワードを入力します。

NMS にトラップを送信するには、**logging history** コマンドを入力します。ロギングをイネーブルにするには、**logging enable** コマンドを使用します。

例

次に、SNMP をイネーブルにし、SNMP ホストおよびトラップを設定し、トラップをシステム メッセージとして送信する例を示します。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の担当者名を設定します。
snmp-server enable	FWSM で SNMP をイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。
snmp-server location	SNMP サーバ ロケーション ストリングを設定します。

snmp-server host

FWSM で SNMP（簡易ネットワーク管理プロトコル）を使用できる NMS 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 **snmp-server host** コマンドを使用します。NMS 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。

snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

no snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

シンタックスの説明

community *text*	この NMS のコミュニティ ストリングを設定します。
host	トラップの送信先または SNMP 要求の受信元となる NMS の IP アドレスを指定します。
interface_name	NMS が FWSM と通信する場合に経由するインターフェイスの名前を指定します。
ip_address	SNMP トラップの送信先または SNMP 要求の受信元となる NMS の IP アドレスを指定します。
trap	（任意）トラップのみを送信し、現在のホストでブラウジング（ポーリング）を禁止するように指定します。
poll	（任意）現在のホストでブラウジング（ポーリング）を許可し、トラップを送信しないように指定します。
udp-port *udp_port*	（任意）通知の送信先となる UDP ポートを設定します。デフォルトでは、SNMP トラップは UDP ポート 162 で送信されます。
version {**1** | **2c**}	（任意）SNMP 通知バージョンを Version 1 または 2c に設定します。

デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 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。

使用上のガイドライン

最大 32 個の NMS を指定できます。

例

次に、境界インターフェイスに接続された 10.1.2.42 をホストに設定する例を示します。

```
hostname(config)# snmp-server host perimeter 10.1.2.42
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の担当者名を設定します。
snmp-server enable	FWSM で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server location	SNMP サーバ ロケーション ストリングを設定します。

snmp-server listen-port

SNMP（簡易ネットワーク管理プロトコル）要求の待ち受けポートを設定するには、グローバル コンフィギュレーション モードで **snmp-server listen-port** コマンドを使用します。デフォルト ポートに戻すには、このコマンドの **no** 形式を使用します。

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

シンタックスの説明

lport	着信要求が受け入れられるポート。デフォルト ポートは 161 です。

デフォルト

デフォルト ポートは 161 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、待ち受けポートを 192 に設定する例を示します。

```
hostname(config)# snmp-server listen-port 192
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の担当者名を設定します。
snmp-server enable	FWSM で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server location	SNMP サーバ ロケーション ストリングを設定します。

snmp-server location

SNMP（簡易ネットワーク管理プロトコル）に対応する FWSM のロケーションを設定するには、グローバル コンフィギュレーション モードで **snmp-server location** コマンドを使用します。このロケ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。

snmp-server location *text*

no snmp-server location [*text*]

シンタックスの説明

location *text*	セキュリティ アプライアンスのロケーションを指定します。**location** *text* は大文字と小文字を区別する 127 文字以下の文字列です。スペースを含めることができますが、複数のスペースは 1 つのスペースに省略されます。

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
1.1(1)	このコマンドが追加されました。

例

次に、ロケーションを Building 42、Sector 54 に設定する例を示します。

```
hostname(config)# snmp-server location Building 42, Sector 54
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の担当者名を設定します。
snmp-server enable	FWSM で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホスト アドレスを設定します。

split-dns

スプリット トンネルを介して解決されるドメイン リストを入力するには、グループポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。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。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

シンタックスの説明

value *domain-name*	FWSM がスプリット トンネルを介して解決するドメイン名を指定します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストにヌル値を設定して、スプリット DNS リストを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからのスプリット DNS リストの継承を禁止します。

デフォルト

スプリット DNS 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
グループ ポリシー	•	—	•	—	—

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

ドメイン リスト内の各エントリを区切るには、スペースを 1 つ使用します。エントリ数に制限はありませんが、文字列全体が 255 文字を超えることはできません。使用できるのは英数字、ハイフン(-)、およびピリオド（.）のみです。

スプリット トンネリング ドメイン リストをすべて削除するには、引数を指定しないで **no split-dns** コマンドを使用します。このコマンドは、**split-dns none** コマンドを発行して作成されたヌル リストを含めて、設定されたスプリット トンネリング ドメイン リストをすべて削除します。

スプリット トンネリング ドメイン リストがない場合、ユーザはデフォルト グループ ポリシー内のすべてのリストを継承します。ユーザがこのようなスプリット トンネリング ドメイン リストを継承できないようにするには、**split-dns none** コマンドを使用します。

例

次に、グループ ポリシー FirstGroup のスプリット トンネリングを介して解決されるように、ドメイン Domain1、Domain2、Domain3、および Domain4 を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	DNS クエリーにドメイン フィールドがない場合に IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメイン リストを指定します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために FWSM が使用するアクセス リストを識別します。
split-tunnel-policy	IPSec クライアントからのパケットを、条件に応じて IPSec トンネルを介して暗号化形式で転送したり、クリアテキスト形式で特定のネットワーク インターフェイスに転送できるようにします。

split-tunnel-network-list

スプリット トンネリング用のネットワーク リストを作成するには、グループポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワーク 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。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

シンタックスの説明

value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙したアクセス リストを識別します。
none	スプリット トンネリング用のネットワーク リストがないことを示します。FWSM はすべてのトラフィックをトンネリングします。 スプリット トンネリング ネットワーク リストにヌル値を設定して、スプリット トンネリングを禁止します。デフォルト グループ ポリシーまたは指定されたグループ ポリシーからのデフォルト スプリット トンネリング ネットワーク リストの継承を禁止します。

デフォルト

デフォルトでは、スプリット トンネリング ネットワーク リストは存在しません。

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
グループ ポリシー	•	—	•	—	—

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 はネットワーク リストに基づいてスプリット トンネリング判断を行います。ネットワーク リストは、プライベート ネットワークのアドレス リストで構成される標準 ACL（アクセス コントロール リスト）です。

スプリット トンネリング ネットワーク リストをすべて削除するには、引数を指定しないで **no split-tunnel-network-list** コマンドを使用します。このコマンドは、**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含めて、設定されたネットワーク リストをすべて削除します。

スプリット トンネリング ネットワーク リストがない場合、ユーザはデフォルト グループ ポリシーまたは指定されたグループ ポリシー内のすべてのネットワーク リストを継承します。ユーザがこのようなネットワーク リストを継承できないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワーク リストでは、トンネルを介してトラフィックを送信する必要があるネットワークと、トンネリングが不要なネットワークが区別されます。

例

次に、グループ ポリシー FirstGroup のネットワーク リスト FirstList を設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成したり、ダウンロード可能なアクセス リストを使用します。
default-domain	DNS クエリーにドメイン フィールドがない場合に IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメイン リストを指定します。
split-tunnel-policy	IPSec クライアントからのパケットを、条件に応じて IPSec トンネルを介して暗号化形式で転送したり、クリアテキスト形式で特定のネットワーク インターフェイスに転送できるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーからスプリット トンネリング値を継承できるようになります。

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

シンタックスの説明

excludespecified	トラフィックがクリア形式で送信されるネットワークのリストを定義します。この機能は、トンネルを介して企業ネットワークに接続されているローカル ネットワーク上のデバイス（プリンタなど）に、リモート ユーザがアクセスする場合に役立ちます。このオプションは、Cisco VPN クライアントにのみ適用されます。
split-tunnel-policy	トラフィックのトンネリング ルールが設定されていることを示します。
tunnelall	トラフィックがクリア形式で送信されないように、あるいは FWSM 以外の宛先に送信されないように指定します。リモート ユーザは企業ネットワークを介してインターネット ネットワークに接続します。ローカル ネットワークにはアクセスできません。
tunnelspecified	指定されたネットワークに対するすべてのトラフィックをトンネリングします。このオプションを指定すると、スプリット トンネリングがイネーブルになります。これにより、トンネリングするネットワーク アドレス リストを作成できるようになります。その他のすべてのアドレス宛のデータはクリア形式で送信され、リモート ユーザのインターネット サービス プロバイダーでルーティングされます。

デフォルト

デフォルトの tunnelall では、スプリット トンネリング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
グループ ポリシー	•	—	•	—	—

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

スプリット トンネリングの主な機能は、セキュリティ機能でなくトラフィック管理機能です。むしろ、セキュリティを最適化するにはスプリット トンネリングをディセーブルにすることを推奨します。スプリット トンネリングを使用すると、リモートアクセス IPSec クライアントからのパケットを、条件に応じて IPSec トンネルを介して暗号化形式で転送したり、クリアテキスト形式で特定のネットワーク インターフェイスに対して転送できるようになります。スプリットトンネリングがイネーブルの場合、宛先が IPSec トンネルの反対側でないパケットは、暗号化し、トンネルを介して送信し、暗号解除して、最終宛先にルーティングする必要がありません。

このコマンドは、このスプリット トンネリング ポリシーを特定のネットワークに適用します。

例

次に、グループ ポリシー FirstGroup で指定されたネットワークのみをトンネリングするように、スプリット トンネリング ポリシーを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	DNS クエリーにドメイン フィールドがない場合に IPSec クライアントが使用するデフォルト ドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメイン リストを指定します。
split-tunnel-network-list none	スプリット トンネリングに対応したアクセス リストがないことを指定します。すべてのトラフィックはトンネルを経由します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために FWSM が使用するアクセス リストを識別します。

ssh

FWSM に SSH（セキュア シェル）アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。FWSM への SSH アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。このコマンドは IPv4 および IPv6 アドレスをサポートします。

ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

シンタックスの説明

interface	SSH をイネーブルにする FWSM インターフェイス。指定しない場合、SSH は外部インターフェイスを除くすべてのインターフェイスでイネーブルになります。
ip_address	FWSM への SSH 接続を開始することが許可されたホストまたはネットワークの IPv4 アドレス。ホストの場合は、ホスト名も入力できます。
ipv6_address/prefix	FWSM への SSH 接続を開始することが許可されたホストまたはネットワークの IPv6 アドレスおよびプレフィクス
mask	*ip_address* のネットワーク マスク

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
1.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

ssh *ip_address* コマンドは、FWSM への SSH 接続を開始することが許可されたホストまたはネットワークを指定します。コンフィギュレーションに複数の ssh コマンドを含めることができます。このコマンドの **no** 形式を使用すると、コンフィギュレーションから特定の SSH コマンドが削除されます。SSH コマンドをすべて削除するには、**clear configure ssh** コマンドを使用します。

FWSM に SSH を開始する前に、**crypto key generate rsa** コマンドを使用してデフォルト RSA 鍵を生成する必要があります。

次に、FWSM でサポートされているセキュリティ アルゴリズムおよび暗号を示します。

- 3DES および AES 暗号（データ暗号化用）
- HMAC-SHA および HMAC-MD5 アルゴリズム（パケットの整合性を保つ場合）
- RSA 公開鍵アルゴリズム（ホスト認証用）
- Diffie-Hellman Group 1 アルゴリズム（鍵交換用）

次の SSH Version 2 の機能は FWSM でサポートされていません。

- X11 転送
- ポート転送
- SFTP サポート
- Kerberos および AFS チケットの送受信
- データ圧縮

例

次に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH Version 2 接続を受け入れるように内部インターフェイスを設定する例を示します。アイドル セッション タイムアウトは 60 分に、SCP はイネーブルに設定されています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションから SSH コマンドをすべて消去します。
crypto key generate rsa	ID 証明書用の RSA 鍵ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報およびエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションに現在含まれている SSH コマンドを表示します。
ssh scopy enable	FWSM 上でセキュアなコピー サーバをイネーブルにします。
ssh version	SSH Version 1 または SSH Version 2 を使用するように FWSM を制限します。

ssh disconnect

アクティブな SSH（セキュア シェル）セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

シンタックスの説明

session_id	ID 番号で指定された SSH セッションを切断します。

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
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。

使用上のガイドライン

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次に、切断している SSH セッションを表示する例を示します。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	FWSM に対するアクティブ SSH セッションの情報を表示します。
ssh timeout	アイドルな SSH セッションのタイムアウト値を設定します。

ssh scopy enable

FWSM で Secure Copy（SCP）をイネーブルにするには、グローバル コンフィギュレーション モードで **ssh scopy enable** コマンドを使用します。SCP 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。

ssh scopy enable

no ssh scopy enable

シンタックスの説明

このコマンドに引数またはキーワードはありません。

デフォルト

このコマンドには、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)	このコマンドのサポートが追加されました。

使用上のガイドライン

SCP はサーバにのみ実装されます。サーバは SCP の接続を受け入れたり、終了することができますが、開始することはできません。FWSM には次の制約事項があります。

- この SCP ではディレクトリがサポートされていません。リモート クライアントからのアクセスは FWSM 内部ファイルに限定されます。
- SCP を使用する場合、バナーはサポートされません。
- SCP はワイルドカードをサポートしません。
- FWSM ライセンスには、SSH Version 2 接続をサポートする VPN-3DES-AES 機能が必要です。

例

次に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH Version 2 接続を受け入れるように内部インターフェイスを設定する例を示します。アイドル セッション タイムアウトは 60 分に、SCP はイネーブルに設定されています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションから SSH コマンドをすべて消去します。
debug ssh	SSH コマンドのデバッグ情報およびエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションに現在含まれている SSH コマンドを表示します。
ssh	指定されたクライアントまたはネットワークから FWSM への SSH 接続を許可します。
ssh version	SSH Version 1 または SSH Version 2 を使用するように FWSM を制限します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*

no ssh timeout

シンタックスの説明

number	SSH セッションが切断されるまでの非アクティブ期間を分で指定します。有効値は 1 ～ 60 分です。

デフォルト

デフォルトのセッション タイムアウト値は 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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。

使用上のガイドライン

ssh timeout コマンドは、セッションが切断されるまでのアイドル期間（分）を指定します。デフォルト期間は 5 分です。

例

次に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH Version 2 接続のみを受け入れるように内部インターフェイスを設定する例を示します。アイドル セッション タイムアウトは 60 分に、SCP はイネーブルに設定されています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションから SSH コマンドをすべて消去します。
show running-config ssh	実行コンフィギュレーションに現在含まれている SSH コマンドを表示します。
show ssh sessions	FWSM に対するアクティブ SSH セッションの情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version

FWSM で許可される SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** 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。

ssh version {*1* | *2*}

no ssh version [*1* | *2*]

シンタックスの説明

1	SSH Version 1 接続のみがサポートされるように指定します。
2	SSH Version 2 接続のみがサポートされるように指定します。

デフォルト

デフォルトでは、SSH Version 1 と SSH Version 2 が両方ともサポートされます。

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)	このコマンドのサポートが追加されました。

使用上のガイドライン

1 および 2 は、FWSM が限定的に使用する SSH のバージョンを指定します。このコマンドの **no** 形式を使用すると、FWSM はデフォルトの互換モードに戻ります（両方のバージョンを使用できます）。デフォルト値の場合は、FWSM との SSH Version 1 および SSH Version 2 接続を確立できます。

例

次に、IP アドレスが 10.1.1.1 の管理コンソールからの SSH Version 2 接続を受け入れるように内部インターフェイスを設定する例を示します。アイドル セッション タイムアウトは 60 分に、SCP はイネーブルに設定されています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションから SSH コマンドをすべて消去します。
debug ssh	SSH コマンドのデバッグ情報およびエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーションに現在含まれている SSH コマンドを表示します。
ssh	指定されたクライアントまたはネットワークから FWSM への SSH 接続を許可します。

ssl server-version

FWSM がサーバとして動作するときに使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルト（any）に戻すには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、FWSM が受け入れる SSL/TSL のバージョンを制限できます。

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

シンタックスの説明

any	SSL バージョン 2 クライアントの HELLO を受け入れ、SSL バージョン 3 または TSL バージョン 1 のどちらかにネゴシエートします。
sslv3	SSL バージョン 2 クライアントの HELLO を受け入れ、SSL バージョン 3 にネゴシエートします。
sslv3-only	SSL バージョン 3 クライアントのみの HELLO を受け入れ、SSL バージョン 3 のみを使用します。
tlsv1	SSL バージョン 2 クライアントの HELLO を受け入れ、TLS バージョン 1 にネゴシエートします。
tlsv1-only	ＴＬＳ バージョン 1 クライアントのみの HELLO を受け入れ、TLS バージョン 1 のみを使用します。

デフォルト

デフォルト値は **any** 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

ssl server-version コマンドは、HTTPS クライアントがファイアウォール管理のためファイアウォールに直接接続するとき、受け入れられる SSL のバージョンの指定に使用します。FWSM では、このコマンドは WebVPN 機能をサポートしません。

例

次に、FWSM が SSL サーバとして動作するとき、TLSv1 のみを使用して通信するように設定する例を示します。

```
hostname(config)# ssl server-version tlsv1-only
```

static

実際の IP アドレスを対応する IP アドレスにマッピングして、1 対 1 の永続的なアドレス変換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 **static** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

スタティック NAT（ネットワーク アドレス変換）の場合：

static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

no static (*real_ifc*,*mapped_ifc***)** {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

スタティック PAT（ポート アドレス変換）の場合：

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

no static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

シンタックスの説明

access-list *access_list_name*	実際のアドレスおよび宛先アドレス（またはポート）を指定して、NAT の実際のアドレスを識別できます。この機能はポリシー NAT といいます。 アクセス リストで使用されるサブネット マスクは、*mapped_ip* でも使用します。 アクセス リストに追加できるのは、**permit** ステートメントのみです。**eq** 演算子を使用して、アクセス リスト内で実際のポートおよび宛先ポートを指定することもできます。ポリシー NAT は **inactive** または **time-range** キーワードを考慮しません。ポリシー NAT 設定では、すべての ACE（アクセス制御エントリ）がアクティブであるとみなされます。
dns	（任意）このスタティック変換と一致する DNS 応答の A レコード（アドレス レコード）を書き替えます。マッピング先のインターフェイスから実際のインターフェイスに DNS 応答が送信される場合、A レコードはマッピング先の値から実際の値に書き替えられます。逆に、実際のインターフェイスからマッピング先のインターフェイスに DNS 応答が送信される場合、A レコードは実際の値からマッピング先の値に書き替えられます。（注）DNS リライトは、PAT には適用されません。各 A レコードには複数の PAT ルールを適用できるので、使用する PAT ルールが明確ではないためです。
emb_lim	（任意）ホストあたりの最大初期接続数を指定します。デフォルト値は 0 で、初期接続数は無制限です。 初期接続数を制限して、DoS 攻撃から保護することができます。FWSM は初期制限を使用して、TCP 代行受信をトリガーします。これにより、TCP SYN パケットがインターフェイスでフラッディングすることによって発生する DoS 攻撃から内部システムが保護されます。初期接続は、送信元と宛先間で必要なハンドシェイクを終了しなかった接続要求です。

interface	マッピング先のアドレスとしてインターフェイスの IP アドレスを使用します。 （注）　スタティック PAT エントリにインターフェイスの IP アドレスを追加する場合は、実際の IP アドレスを指定しないで、interface キーワードを使用する必要があります。
mapped_ifc	マッピング先の IP アドレス ネットワークに接続されたインターフェイスの名前を指定します。
mapped_ip	実際のアドレスの変換先アドレスを指定します。
mapped_port	マッピング先の TCP または UDP ポートを指定します。ポートはリテラル名、または 0 ～ 65535 のポート番号で指定できます。 有効なポート番号は、次の Web サイトからオンラインで表示することができます。 http://www.iana.org/assignments/port-numbers
netmask *mask*	実際のアドレスおよびマッピング アドレスのサブネット マスクを指定します。単一ホストの場合は、255.255.255.255 を使用します。マスクを入力しない場合は、1 つの例外を除いて、IP アドレス クラスのデフォルト マスクが使用されます。マスク後のホストビットがゼロでない場合にかぎり、ホスト マスクには 255.255.255.255 が使用されます。*real_ip* ではなく **access-list** キーワードを使用した場合は、アクセス リストで使用したサブネット マスクが *mapped_ip* にも使用されます。
norandomseq	（任意）TCP ISN ランダム化の保護機能をディセーブルにします。別のインライン ファイアウォールで TCP シーケンス番号のランダム化をイネーブルにしている場合は、ランダム化をディセーブルにできます。2 つのファイアウォールで同じ動作を実行する必要はないからです。ただし、ISN ランダム化については、両方のファイアウォールでイネーブルのままにしても、トラフィックに影響はありません。 各 TCP 接続には ISN が 2 つあります。1 つはクライアントによって生成され、もう 1 つはサーバによって生成されます。セキュリティ アプライアンスは、発信方向に渡される TCP SYN の ISN をランダム化します。同一セキュリティ レベルの 2 つのインターフェイス間の接続では、SYN の ISN が両方向でランダム化されます。 保護されたホストで ISN をランダム化すると、新規接続の次の ISN を予測して新規セッションをハイジャックする攻撃を阻止できます。 **norandomseq** キーワードは外部 NAT には適用されません。ファイアウォールがランダム化するのは、セキュリティがより高いインターフェイス上のホスト / サーバで生成される ISN のみです。外部 NAT に norandomseq を設定しても、**norandomseq** キーワードは無視されます。
real_ifc	実際の IP アドレス ネットワークに接続されたインターフェイスの名前を指定します。
real_ip	変換する実際のアドレスを指定します。
real_port	実際の TCP または UDP ポートを指定します。ポートはリテラル名、または 0 ～ 65535 のポート番号で指定できます。 有効なポート番号は、次の Web サイトからオンラインで表示することができます。 http://www.iana.org/assignments/port-numbers

tcp	スタティック PAT の場合は、プロトコルに TCP を指定します。
tcp *max_conns*	各 real_ip 可変ホストが使用を許可される同時 TCP 接続の最大数を指定します。デフォルト値は 0 で、接続数は無制限です（**timeout conn** コマンドで指定されたアイドル タイムアウトが経過すると、アイドル接続は終了します）。
udp	スタティック PAT の場合は、プロトコルに UDP を指定します。
udp *udp_max_conns*	（任意）サブネット全体における同時 UDP 接続の最大数を指定します。デフォルト値は 0 で、接続数は無制限です（**timeout conn** コマンドで指定されたアイドル タイムアウトが経過すると、アイドル接続は終了します）。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は、使用可能な最大値を示す 0（無制限）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。
2.2(1)	ローカル ホストの UDP 最大接続数をサポートするように、このコマンドが変更されました。

使用上のガイドライン

スタティック NAT は、実際のアドレスからマッピング アドレスへの固定的な変換を行います。ダイナミック NAT および PAT は、以降の変換を行うたびに、各ホストは異なるアドレスまたはポートを使用します。スタティック NAT では、連続するどの接続でもマッピング アドレスが同じで、変換ルールは永続的であるため、宛先ネットワークのホストから変換先ホストにトラフィックを送信できます（この処理を許可するアクセス リストがある場合）。

ダイナミック NAT とスタティック NAT のアドレス範囲の主な違いは、スタティック NAT では、リモート ホストから変換先ホストへの接続を開始でき（この処理を許可するアクセス リストがある場合）、ダイナミック NAT ではこれができないことです。スタティック NAT の場合は、実際のアドレスと同数のマッピング アドレスも必要です。

スタティック PAT はスタティック NAT と同じです。ただし、スタティック PAT では、実際のアドレスとマッピング アドレスのプロトコル（TCP または UDP）およびポートを指定することができます。

この機能によって、複数の異なるスタティック ステートメントについて同じマッピング アドレスを指定することができます。ただし、ステートメントごとにポートは異なっている必要があります。

同じ 2 つのインターフェイス間で複数の **static** コマンドを実行する場合は、実際のアドレスまたはマッピング アドレスに同じ値を使用できません。**global** コマンドで定義されたマッピング アドレスを、同じマッピング先のインターフェイスに対する **static** コマンド内で使用しないでください。

セカンダリ チャネル（FTP［ファイル転送プロトコル］、VoIP など）のアプリケーション検査が必要となるアプリケーションの場合、ポリシー NAT 内でポートを指定すると、セカンダリ ポートが自動的に変換されます。

NAT は、一般に、トランスペアレント ファイアウォール モードで使用できません。トランスペアレント ファイアウォール モードでは、***static*** コマンドを使用して、最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定できます。この場合、実際の IP アドレスとマッピング先 IP アドレスは同じです。

Modular Policy Framework を使用して、接続制限を設定することもできます（ただし、初期接続制限は設定できません）。詳細については、**set connection** コマンドを参照してください。初期接続制限を設定するには、NAT を使用する必要があります。両方の方法を使用して同じトラフィックにこれらの設定値を設定した場合は、小さい方の値が使用されます。TCP シーケンス ランダム化は、いずれかの方法を使用してディセーブルになっていれば、ディセーブルになります。

変換用ネットワーク（10.1.1.0 255.255.255.0 など）を指定すると、.0 および .255 アドレスが変換されます。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセス リストを設定してください。

static コマンド ステートメントを変更または削除した場合は、**clear xlate** コマンドを使用して、変換を消去します。

例

スタティック NAT の例

たとえば、次のポリシー スタティック NAT の例では、単一の実際のアドレスが、宛先アドレスに応じて 2 つのマッピング アドレスに変換されます。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドは、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）にマッピングします。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255
```

次のコマンドは、外部 IP アドレス（209.165.201.15）を内部 IP アドレス（10.1.1.6）にマッピングします。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

次のコマンドは、サブネット全体をスタティックにマッピングします。

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

次に、Intel Internet Phone、CU-SeeMe、CU-SeeMe Pro、MeetingPoint、または Microsoft NetMeeting を使用して、H.323 を介して無制限のユーザにコールできるようにする例を示します。**static** コマンドはアドレス 209.165.201.0 ～ 209.165.201.30 をローカル アドレス 10.1.1.0 ～ 10.1.1.30 にマッピングします（209.165.201.1 は 10.1.1.1 に、209.165.201.10 は 10.1.1.10 にマッピングします）。

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask
255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq
h323
hostname(config)# access-group acl_out in interface outside
```

次に、Mail Guard をディセーブルにするために使用されるコマンドの例を示します。

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

この例では、**static** コマンドを使用して、外部ホストから dmz1 インターフェイス上の 10.1.1.1 メール サーバ ホストへのアクセスを許可するように、グローバル アドレスを設定できます。209.165.201.1 アドレスを指すように DNS の MX レコードを設定して、メールがこのアドレスに送信されるようにする必要があります。**access-list** コマンドを使用すると、外部ユーザは SMTP ポート（25）を介してグローバル アドレスにアクセスできます。**no fixup protocol** コマンドは Mail Guard をディセーブルにします。

スタティック PAT の例

たとえば、10.1.3.0 ネットワーク上のホストから FWSM の外部インターフェイス（10.1.2.14）に送信された Telnet トラフィックを 10.1.1.15 の内部ホストにリダイレクトするには、次のコマンドを使用します。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

10.1.3.0 ネットワーク上のホストから FWSM の外部インターフェイス（10.1.2.14）に送信された HTTP トラフィックを 10.1.1.15 の内部ホストにリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

FWSM の外部インターフェイス（10.1.2.14）から 10.1.1.15 の内部ホストに Telnet トラフィックをリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
```

ただし、上記の実際の Telnet サーバから接続を開始できるようにするには、追加変換を設定する必要があります。たとえば、その他のすべてのタイプのトラフィックを変換するには、次のコマンドを入力します。元の **static** コマンドはサーバに Telnet 変換を実行しますが、**nat** および **global** コマンドはサーバからの発信接続に PAT を実行します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

すべての内部トラフィックに個別の変換を設定し、内部ホストで Telnet サーバと異なるマッピング アドレスを使用している場合は、サーバへの Telnet トラフィックを許可する **static** ステートメントと同じマッピング アドレスを使用するように、Telnet サーバから送信されるトラフィックを設定することができます。Telnet サーバに限っては、より限定的な **nat** ステートメントを作成する必要があります。**nat** ステートメントは最適一致を検索するために読み込まれるため、より限定的な **nat** ステートメントは一般のステートメントよりも先に照合されます。次に、Telnet **static** ステートメント、Telnet サーバから送信されたトラフィックに対する、より限定的な **nat** ステートメント、および別のマッピング アドレスを使用するその他の内部ホストのステートメントの例を示します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

既知のポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

関連コマンド

コマンド	説明
clear configure static	コンフィギュレーションから **static** コマンドを削除します。
clear xlate	すべての変換を削除します。
nat	ダイナミック NAT を設定します。
show running-config static	コンフィギュレーション内の **static** コマンドをすべて表示します。
timeout conn	接続のタイムアウトを設定します。

strict-http

準拠しない HTTP トラフィックを転送できるようにするには、HTTP マップ コンフィギュレーション モードで **strict-http** 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。この機能をデフォルト動作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。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no strict-http action {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に失敗した場合に実行するアクション
allow	メッセージを許可します。
drop	接続を終了します。
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て、接続を閉じます。

デフォルト

このコマンドは、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

厳格な HTTP 検査をディセーブルにすることはできませんが、**strict-http action allow** コマンドを実行すると FWSM は準拠しない HTTP トラフィックを転送できるようになります。このコマンドは、準拠しない HTTP トラフィックの転送を禁止するデフォルト動作を無効にします。

例

次に、準拠しない HTTP トラフィックの転送を許可する例を示します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
```

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。

strip-group

このコマンドは、user@realm 形式で受信したユーザ名にのみ適用されます。レルムは、ユーザ名に @ デリミタが付加された管理ドメインです（juser@abc）。

strip-group 処理をイネーブルまたはディセーブルにするには、tunnel-group general-attributes モードで **strip-group** コマンドを使用します。FWSM は VPN（バーチャル プライベート ネットワーク）クライアントが提示したユーザ名からグループ名を取得して、PPP（ポイントツーポイント）接続用のトンネル グループを選択します。strip-group 処理がイネーブルの場合、FWSM はユーザ名のユーザ部分のみを送信して許可または認証を行います。それ以外の場合（strip-group 処理がディセーブルの場合）、FWSM はレルムを含むユーザ名全体を送信します。

strip-group 処理をディセーブルにするには、このコマンドの ***no*** 形式を使用します。

strip-group

no strip-group

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定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
tunnel-group general-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

この属性を適用できるのは、IPSec リモート アクセスおよび L2TP/IPSec トンネルタイプのみです。

例

次に、リモート アクセス トンネル グループ [remotegrp] のタイプを IPSec リモート アクセスに設定し、一般コンフィギュレーション モードを開始し、トンネル グループ [remotegrp] をデフォルト グループ ポリシーに設定し、このトンネル グループに対して strip-group をイネーブルにする例を示します。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-group
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。
group-delimiter	グループ名解析をイネーブルにし、トンネルのネゴシエーション中に受信されたユーザ名からグループ名を解析する場合に使用するデリミタを指定します。
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 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。

strip-realm

strip-realm 処理をイネーブルまたはディセーブルにするには、tunnel-group general-attributes コンフィギュレーション モードで **strip-realm** コマンドを使用します。strip-realm 処理では、認証サーバまたは許可サーバにユーザ名を送信するときに、ユーザ名からレルムが除去されます。レルムは、ユーザ名に @ デリミタが付加された管理ドメインです（username@realm）。このコマンドがイネーブルの場合、FWSM はユーザ名のユーザ部分のみを送信して許可または認証を行います。それ以外の場合、FWSM はユーザ名全体を送信します。

strip-realm 処理をディセーブルにするには、このコマンドの ***no*** 形式を使用します。

strip-realm

no strip-realm

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

このコマンドのデフォルト設定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
tunnel-group general-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

この属性を適用できるのは、IPSec リモート アクセス トンネルタイプのみです。

例

次に、リモート アクセス トンネル グループ [remotegrp] のタイプを IPSec リモート アクセスに設定し、一般コンフィギュレーション モードを開始してトンネル グループ [remotegrp] をデフォルト グループ ポリシーに設定し、このトンネル グループに対して strip-realm をイネーブルにする例を示します。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-realm
```

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	指定された証明書マップ エントリを表示します。
tunnel-limit	**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。

subject-name (crypto ca certificate map)

IPSec ピア証明書のサブジェクト DN にルール エントリを適用するように指定するには、CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag*] {**eq | ne | co | nc**} *string*

no subject-name [**attr** *tag*] {**eq | ne | co | nc**} *string*

シンタックスの説明

attr tag	（任意）証明書 DN の指定された属性値のみをルール エントリの文字列と比較するように指定します。tag の値は次のとおりです。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 姓 IP = IP アドレス SER = シリアル番号 UNAME = 構造化されていない名前 EA = 電子メール アドレス T = 肩書き O = 組織名 L = 地名 SP = 州 / 県 C = 国 OU = 組織単位 CN = 一般名称
co	ルール エントリの文字列が DN 文字列または指定された属性に含まれている必要があります。
eq	DN 文字列または指定された属性がルール文字列全体と一致する必要があります。
nc	ルール エントリ文字列が DN 文字列または指定された属性に含まれていない必要があります。
ne	DN 文字列または指定された属性がルール文字列全体と一致しない必要があります。
string	比較する値を指定します。

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
暗号 CA 証明書マップ 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。

例

次に、証明書マップ 1 に対して CA 証明書マップ モードを開始して、証明書サブジェクト名の組織属性が Central と一致する必要があることを示すルール エントリを作成する例を示します。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
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。
issuer-name	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	**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。

subject-name (crypto ca trustpoint)

指定されたサブジェクト DN を登録中の証明書に追加するには、crypto ca トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。このサブジェクト名は、証明書を使用する人物またはシステムです。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

subject-name *X.500_name*

no subject-name

シンタックスの説明

X.500_name	X.500 で識別される名前を定義します。たとえば、cn=crl,ou=certs,o=CAName,c=US のように定義します。最大文字長は 1 K です（事実上無制限です）。

デフォルト

デフォルト設定では、サブジェクト名を含めません。

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
crypto ca トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、トラストポイント central に対して crypto ca トラストポイント コンフィギュレーション モードを開始して、URL https//:www.example.com に自動登録を設定し、トラストポイント central の登録要求にサブジェクト DN OU cisco.example を追加する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://www.example.com/
hostname(ca-trustpoint)# subject-name ou=cisco.example
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment url	CA を使用して登録する URL を指定します。

summary-address

OSPF の集約アドレスを作成するには、ルータ コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプションを削除するには、このコマンドの **no** 形式を使用します。

summary-address *addr mask* [***not-advertise***] [***tag*** *tag_value*]

no summary-address *addr mask* [***not-advertise***] [***tag*** *tag_value*]

シンタックスの説明

addr	アドレス範囲用に指定する集約アドレスの値
mask	サマリー ルートに使用する IP サブネット マスク
not-advertise	（任意）指定したプレフィクス / マスクのペアと一致するルートを抑制します。
tag *tag_value*	（任意）各外部ルートに結合する 32 ビット 10 進値。OSPF 自体はこの値を使用しません。この値は、ASBR 間で情報を伝達する場合に使用します。値を指定しない場合、BGP および EGP からのルートにはリモート Autonomous System（AS; 自律システム）の番号が使用され、他のプロトコルの場合にはゼロ（0）が使用されます。有効値は 0 ～ 4294967295 です。

デフォルト

デフォルトの設定は次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィクス / マスクのペアと一致するルートは抑制されません。

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
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

他のルーティング プロトコルから学習したルートをサマライズできます。OSPF にこのコマンドを使用すると、OSPF Autonomous System Boundary Router（ASBR）は、アドレスがカバーするすべての再配信済みルートの集約ルートとして、1 つの外部ルートをアドバタイズできます。このコマンドは、OSPF に再配信されているその他のルーティング プロトコルからのルートのみをサマライズします。OSPF エリア間のルートをサマライズするには、**area range** コマンドを使用します。

コンフィギュレーションから **summary-address** コマンドを削除するには、オプションのキーワードまたは引数を指定しないで、このコマンドの no 形式を使用します。コンフィギュレーションの summary コマンドからオプションを削除するには、削除するオプションを指定して、このコマンドの **no** 形式を使用します。詳細については、「例」を参照してください。

例

次に、3 に設定された ***tag*** 値を使用して、ルート サマライズを設定する例を示します。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次に、オプションを含む **summary-address** コマンドの **no** 形式を使用して、このオプションをデフォルト値に戻す例を示します。この例では、上記の例で 3 に設定された ***tag*** 値が **summary-address** コマンドから削除されます。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次に、コンフィギュレーションから **summary-address** コマンドを削除する例を示します。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
area range	エリア境界でルートを統合し、サマライズします。
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 summary-address	OSPF ルーティング プロセスごとに、サマリー アドレス設定を表示します。

sunrpc-server

SunRPC サービス テーブルにエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。コンフィギュレーションから SunRPC サービス テーブルを削除するには、このコマンドの **no** 形式を使用します。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **{protocol** {**tcp** | **udp}} **port** *port* [**-** *port*]
timeout *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **{protocol** {**tcp** | **udp}} **port** *port* [**-** *port*]
timeout *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

シンタックスの説明

ifc_name	サーバ インターフェイス名
ip_addr	SunRPC サーバの IP アドレス
mask	ネットワーク マスク
port *port* [**-** *port*]	SunRPC プロトコル ポート範囲を指定します。
protocol tcp	SunRPC トランスポート プロトコルを指定します。
protocol udp	SunRPC トランスポート プロトコルを指定します。
service *service_type*	SunOS **rpcinfo** コマンドの出力で指定されているとおりに、SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックのアクセスが終了するまでのタイムアウト アイドル時間を指定します。

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
2.2(1)	**rpc-server** コマンドが追加されました。
3.1(1)	このコマンドは **rpc-server** から変更されました。

使用上のガイドライン

SunRPC サービス テーブルは、timeout で指定された期間中に確立された SunRPC セッションに基づいて、FWSM 内の SunRPC トラフィックの通過を許可する場合に使用します。

例

次に、SunRPC サービス テーブルを作成する例を示します。

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	FWSM から Sun リモート プロセッサ コール サービス を消去します。
show running-config sunrpc-server	SunRPC の設定に関する情報を表示します。

support-user-cert-validation

リモート証明書を発行した CA に対して現在のトラストポイントが認証される場合に、このトラストポイントに基づいてリモート ユーザ証明書を検証するには、crypto ca トラストポイント コンフィギュレーション モードで **support-user-cert-validation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

support-user-cert-validation

no support-user-cert-validation

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルト設定では、ユーザ証明書の検証がサポートされます。

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
crypto ca トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
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、同じ CA を持つトラストポイントを 2 つ設定できるため、同じ CA から 2 つの異なる ID 証明書が生成されます。トラストポイントの認証先 CA に、この機能がイネーブル化された別のトラストポイントがすでに対応付けられている場合は、このオプションが自動的にディセーブルになります。これにより、パス検証パラメータがあいまいに選択されることがなくなります。トラストポイントの認証先 CA に、この機能がイネーブル化された別のトラストポイントがすでに対応付けられている場合、ユーザがこの機能を実行しようとしてもアクションは許可されません。2 つのトラストポイントでこの設定をイネーブルにして、同じ CA に対して認証することはできません。

例

次に、トラストポイント central に対して crypto ca トラストポイント コンフィギュレーション モードを開始して、トラストポイント central でのユーザ検証をイネーブルにする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルトに戻します。

sysopt connection tcpmss

最大 TCP セグメント サイズが設定値を超えたり、最大値が指定サイズを下回らないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sysopt connection tcpmss [***minimum***] *bytes*

no sysopt connection tcpmss [***minimum***] [*bytes*]

シンタックスの説明

bytes	最大 TCP セグメント サイズをバイト数で指定します（48 から最大値までの値）。デフォルト値は 1380 バイトです。この機能をディセーブルにするには、*bytes* を 0 に設定します。 ***minimum*** キーワードを指定した場合、*bytes* は許可されている最小の最大値を表します。
minimum	（任意）最大セグメント サイズが *bytes*（48 ～ 65535 バイト）以上の値になるように上書きします。この機能は、デフォルトでディセーブルです（0 に設定）。

デフォルト

デフォルトの最大値は 1380 バイトです。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

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。

使用上のガイドライン

ホストとサーバは両方とも、最初に接続を確立するときに最大セグメント サイズを設定できます。いずれかの最大値が **sysopt connection tcpmss** コマンドで設定された値よりも大きい場合、FWSM は最大値を無効にして、設定された値を挿入します。いずれかの最大値が **sysopt connection tcpmss minimum** コマンドで設定された値よりも小さい場合、FWSM は最大値を無効にして、設定された [minimum] 値を挿入します（minimum 値は、実際は使用可能な最小の最大値です）。たとえば、最大サイズに 1200 バイト、最小サイズに 400 バイトが設定してある場合に、ホストが最大サイズとして 1300 バイトを要求すると、FWSM は 1200 バイト（最大値）を要求するようにパケットを変更します。別のホストが最大値として 300 バイトを要求した場合、FWSM は 400 バイト（最小値）を要求するようにパケットを変更します。

デフォルトの 1380 バイトは、合計パケット サイズがイーサネットのデフォルト MTU（最大伝送ユニット）である 1500 バイトを超過しないように、ヘッダー情報分のサイズを確保したサイズです。次の計算を参照してください。

1380 データ＋ 20 TCP ＋ 20 IP ＋ 24 AH ＋ 24 ESP_CIPHER ＋ 12 ESP_AUTH ＋ 20 IP ＝ 1500 バイト

ホストまたはサーバが最大セグメント サイズを要求しない場合、FWSM は RFC 793 のデフォルト値である 536 バイトが有効であると想定します。

1380 を超える最大サイズを設定すると、MTU サイズ（デフォルトは 1500）に応じてパケットが分割されることがあります。分割数が多いと、フラグ ガード機能を使用する場合に、FWSM のパフォーマンスが低下することがあります。最小サイズを設定すると、TCP サーバがクライアントに多数の小さな TCP データ パケットを送信することでサーバおよびネットワークのパフォーマンスが低下することがなくなります。

（注） この機能を通常使用することは推奨しませんが、Syslog IPFRAG メッセージ 209001 および 209002 が表示された場合は、*bytes* 値を大きくすることができます。

例

次に、最大サイズを 1200 に、最小値を 400 に設定する例を示します。

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドの設定を消去します。
show running-config sysopt	**sysopt** コマンドの設定を表示します。
sysopt connection timewait	最後の標準 TCP 停止シーケンス後も、各 TCP 接続が短縮された TIME_WAIT 状態にとどまるように設定します。

sysopt nodnsalias

DNS 検査をディセーブルにして、**alias** コマンドを使用したときに DNS A レコード アドレスが変更されないようにするには、グローバル コンフィギュレーション モードで **sysopt nodnsalias** 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。**alias** コマンドで NAT（ネットワーク アドレス変換）のみを実行し、DNS パケット変換が不要な場合は、DNS アプリケーション検査をディセーブルにすることができます。

sysopt nodnsalias {*inbound* | *outbound*}

no sysopt nodnsalias {*inbound* | *outbound*}

シンタックスの説明

inbound	セキュリティの低いインターフェイスから、**alias** コマンドで指定されたセキュリティの高いインターフェイスに送信されるパケットに対して、DNS レコード変更をディセーブルにします。
outbound	**alias** コマンドで指定されたセキュリティの高いインターフェイスからセキュリティの低いインターフェイスに送信されるパケットに対して、DNS レコード変更をディセーブルにします。

デフォルト

デフォルトでは、この機能はディセーブルです（DNS レコード アドレスは変更できます）。

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
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

alias コマンドは NAT を実行して DNS A レコード アドレスを変更します。場合によっては、DNS レコード変更をディセーブルにすることができます。

例

次に、着信パケットの DNS アドレス変更をディセーブルにする例を示します。

```
hostname(config)# sysopt nodnsalias inbound
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換を反映するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドの設定を消去します。
show running-config sysopt	**sysopt** コマンドの設定を表示します。
sysopt noproxyarp	インターフェイス上でプロキシ ARP をディセーブルにします。

sysopt noproxyarp

インターフェイス上で NAT（ネットワーク アドレス変換）グローバル アドレスのプロキシ ARP をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt noproxyarp** コマンドを使用します。グローバル アドレスのプロキシ ARP を再イネーブルにするには、このコマンドの **no** 形式を使用します。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

シンタックスの説明

interface_name	プロキシ ARP をディセーブルにするインターフェイスの名前を指定します。

デフォルト

グローバル アドレスのプロキシ ARP は、デフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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。

使用上のガイドライン

まれに、グローバル アドレスのプロキシ ARP をディセーブルにしなければならない場合があります。

同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信するホストでは、このデバイスの MAC（メディア アクセス制御）アドレス情報が必要です。ARP は、IP アドレスから MAC アドレスへの変換を解決するレイヤ 2 プロトコルです。ホストが「この IP アドレスの所有者は誰か？」を確認する ARP 要求を送信すると、この IP アドレスを所有するデバイスが「自分がこの IP アドレスを持っていて、MAC アドレスは次のとおりである」と応答します。

プロキシ ARP は、デバイスがこの IP アドレスを所有していない場合でも、ARP 要求に自身の MAC アドレスで応答する場合に使用します。ユーザが NAT を設定し、FWSM インターフェイスと同じネットワーク上のグローバル アドレスを指定した場合、FWSM はプロキシ ARP を使用します。トラフィックがホストに到達するには、FWSM がプロキシ ARP を使用して、FWSM MAC アドレスが宛先グローバル アドレスに割り当てられていることを示す必要があります。

例

次に、内部インターフェイスでプロキシ ARP をディセーブルにする例を示します。

```
hostname(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換を反映するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドの設定を消去します。
show running-config sysopt	**sysopt** コマンドの設定を表示します。
sysopt nodnsalias	**alias** コマンドを使用する場合に、DNS A レコード アドレスの変更を禁止します。

sysopt radius ignore-secret

RADIUS アカウンティング応答内の認証鍵を無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** 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。一部の RADIUS サーバとの互換性を保つために、認証鍵を無視しなければならない場合があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでディセーブルです。

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
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。

使用上のガイドライン

Livingston Version 1.16 など、鍵をアカウンティング確認応答内の認証ハッシュに含めない一部の RADIUS サーバでは、使用時に注意する必要があります。この場合、FWSM がアカウンティング要求を再送信し続けることがあります。アカウンティング確認応答の認証者の鍵を無視して、再送信問題を回避するには、**sysopt radius ignore-secret** コマンドを使用します（ここで説明している鍵は、**aaa-server host** コマンドで設定された鍵です）。

例

次に、アカウンティング応答内の認証鍵を無視する例を示します。

```
hostname(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを識別します。
clear configure sysopt	**sysopt** コマンドの設定を消去します。
show running-config sysopt	**sysopt** コマンドの設定を表示します。

sysopt uauth allow-http-cache

Web ブラウザが FWSM の仮想 HTTP サーバを使用して再認証する場合に（**virtual http** コマンドを参照）、キャッシュ内のユーザ名およびパスワードを提供できるようにするには、グローバル コンフィギュレーション モードで **sysopt uauth allow-http-cache** コマンドを使用します。HTTP キャッシュを禁止する場合は、認証セッションがタイムアウトしたあと、次に仮想 HTTP サーバに接続するときに、ユーザ名およびパスワードが再要求されます。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。

sysopt uauth allow-http-cache

no sysopt uauth allow-http-cache

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

この機能は、デフォルトでディセーブルです。

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
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、HTTP キャッシュの使用を許可する例を示します。

```
hostname(config)# sysopt uauth allow-http-cache
```

関連コマンド

コマンド	説明
virtual http	FWSM 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、FWSM および HTTP サーバで別々に認証することができます。仮想 HTTP を使用しない場合、FWSM での認証に使用したのと同じユーザ名およびパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名およびパスワードが別に要求されることはありません。
clear configure sysopt	**sysopt** コマンドの設定を消去します。
show running-config sysopt	**sysopt** コマンドの設定を表示します。