activation-key ～ auto-update timeout コマンド

activation-key

FWSM のアクティベーション キーを変更し、FWSM 上で運用されているアクティベーション キーを、FWSM のフラッシュ メモリに非表示のファイルとして保存されているアクティベーション キーと比較してチェックするには、グローバル コンフィギュレーション モードで **activation-key** コマンドを使用します。

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

シンタックスの説明

activation-key-four-tuple	アクティベーション キーを設定します。表記上の注意点については「使用上のガイドライン」を参照してください。
activation-key-five-tuple	アクティベーション キーを設定します。表記上の注意点については「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにはデフォルト設定はありません。

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)	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

次のように、4 つの要素で構成される 16 進文字列で、各要素の間にスペースを 1 つ入れて *activation-key-four-tuple* を入力するか、5 つの要素で構成される 16 進文字列で、各要素の間にスペースを 1 つ入れて *activation-key-five-tuple* を入力します。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭部分の 0x 指定子は省略できます。値はすべて 16 進数であるとみなされます。

キーはコンフィギュレーション ファイルには保管されません。キーはシリアル番号に関連付けられます。

例

次に、FWSM でアクティベーション キーを変更する例を示します。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

関連コマンド

コマンド	説明
show activation-key	アクティベーション キーを表示します。

address-pool

リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定するには、tunnel-group general-attributes コンフィギュレーション モードで **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの ***no*** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

シンタックスの説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 つまでローカル アドレス プールを指定できます。
interface name	（任意）アドレス プールで使用するインターフェイスを指定します。

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 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

各インターフェイスにこれらのコマンドを複数入力できます。インターフェイスを指定しないと、コマンドによって、明示的に言及していないすべてのインターフェイスにデフォルトが指定されます。

例

次に、config-general コンフィギュレーション モードで、IPSec リモート アクセス トンネル グループ xyz のリモート クライアントにアドレスを割り当てるために、アドレス プールのリストを指定する例を示します。

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモート アクセス トンネルで使用する IP アドレス プールを設定します。
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 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。

admin-context

システム コンフィギュレーションの管理コンテキ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 **admin-context** コマンドを使用します。システムのコンフィギュレーションには、ネットワーク インターフェイスまたはコンフィギュレーションのネットワーク設定が含まれておらず、システムがネットワーク リソースにアクセスする必要がある場合（FWSM ソフトウェアをダウンロードする場合、または管理者のリモート管理を許可する場合）、管理コンテキストとして指定されているコンテキストの 1 つを使用します。

admin-context *name*

シンタックスの説明

name	名前として、32 文字までの長さのテキスト文字列を設定します。コンテキストをまだ定義していない場合は、まずこのコマンドを使用して管理コンテキストの名前を指定します。そして、**context** コマンドを使用して追加する最初のコンテキストが指定した管理コンテキスト名である必要があります。 この名前は大文字と小文字が区別されるので、たとえば、[customerA] と [CustomerA] という名前の 2 つのコンテキストを設定できます。文字、数字、またはハイフンを使用できますが、ハイフンで名前を開始または終了することはできません。 [System] または [Null]（大文字または小文字）は予約名なので、使用できません。

デフォルト

マルチ コンテキスト モードの新しい FWSM では、管理コンテキストが「管理者（admin）」と呼ばれます。

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	該当なし	該当なし	—	—	•

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

コンテキストのコンフィギュレーションが内部フラッシュ メモリに存在するかぎり、任意のコンテキストを管理コンテキストに設定できます。

clear configure context コマンドを使用してすべてのコンテキストを削除する場合を除いて、現在の管理コンテキストを削除できません。

例

次に、管理コンテキストを [administrator] に設定する例を示します。

```
hostname(config)# admin-context administrator
```

関連コマンド

コマンド	説明
clear configure context	システムのコンフィギュレーションからすべてのコンテキストを削除します。
context	システム コンフィギュレーションでコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show admin-context	現在の管理コンテキスト名を表示します。

alias

手動でアドレスを変換して、DNS 応答を変更するには、グローバル コンフィギュレーション モードで **alias** コマンドを使用します。**alias** コマンドを削除するには、このコマンドの **no** 形式を使用します。このコマンドの機能は、**dns** キーワードを指定した **nat** コマンドと **static** コマンドを含む、外部 NAT コマンドに置き換えられています。**alias** コマンドではなく、外部 NAT を使用することを推奨します。

alias *interface_name mapped_ip real_ip* [*netmask*]

[no] alias *interface_name mapped_ip real_ip* [*netmask*]

シンタックスの説明

interface_name	マッピング IP アドレス宛てのトラフィックの入力側インターフェイス名（またはマッピング IP アドレスからのトラフィックの出力側インターフェイス名）を指定します。
mapped_ip	実際の IP アドレスの変換先となる IP アドレスを指定します。
real_ip	実際の IP アドレスを指定します。
netmask	（任意）両方の IP アドレスのサブネット マスクを指定します。ホスト マスクには、**255.255.255.255** を入力します。

デフォルト

このコマンドにはデフォルト設定はありません。

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

このコマンドは、宛先アドレスのアドレス変換を実行する場合にも使用できます。たとえば、ホストがパケットを 209.165.201.1 に送信する場合は、**alias** コマンドを使用することで、トラフィックをほかのアドレス（209.165.201.30 など）にリダイレクトできます。

（注）　***alias*** コマンドが他のアドレスの変換ではなく、DNS の書き換えに使用される場合は、エイリアス対応のインターフェイスで ***proxy-arp*** をディセーブルにします。***proxy-arp*** によって FWSM が一般的な NAT 処理でトラフィックを自身に引き寄せるのを避けるには、***sysopt noproxyarp*** コマンドを使用します。

alias コマンドを変更または削除したら、**clear xlate** コマンドを使用します。

DNS ゾーン ファイルの中に、**alias** コマンドに含まれている [dnat] アドレスの A（アドレス）レコードが存在している必要があります。

alias コマンドには 2 つの使用方法があります。次にその概略を示します。

- FWSM が *mapped_ip* 宛てのパケットを取得した場合に、**alias** コマンドを使用して、そのパケットを *real_ip* に送信するように設定できます。
- FWSM が FWSM に戻された *real_ip* 宛ての DNS パケットを取得した場合に、**alias** コマンドを使用して DNS パケットを変更し、宛先ネットワークのアドレスを *mapped_ip* に変更するように設定できます。

alias コマンドは、ネットワーク上の DNS サーバと自動的に対話して、エイリアスが設定された IP アドレスへのドメイン名によるアクセスを透過的に処理します。

real_ip と *mapped_ip* IP アドレスのネットワーク アドレスを使用すると、ネット エイリアスを指定できます。たとえば、**alias 192.168.201.0 209.165.201.0 255.255.255.224** コマンドを実行すると、209.165.201.1 ～ 209.165.201.30 の各 IP アドレスのエイリアスが作成されます。

static コマンドおよび **access-list** コマンドで **alias** *mapped_ip* アドレスにアクセスするには、**access-list** コマンドの中で、許可されるトラフィック発信元アドレスとして *mapped_ip* アドレスを指定します。次に例を示します。

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1
eq ftp-data
hostname(config)# access-group acl_out in interface outside
```

内部アドレス 192.168.201.1 を宛先アドレス 209.165.201.1 にマッピングして、エイリアスを指定しています。

内部ネットワーク クライアント 209.165.201.2 が example.com に接続すると、内部クライアントのクエリーに対する外部 DNS サーバからの DNS 応答は、FWSM によって 192.168.201.29 へと変更されます。FWSM で 209.165.200.225 ～ 209.165.200.254 をグローバル プール IP アドレスとして使用している場合、パケットは FWSM に SRC=209.165.201.2 および DST=192.168.201.29 として送信されます。FWSM は、アドレスを外部の SRC=209.165.200.254 および DST=209.165.201.29 に変換します。

例

次の例では、内部ネットワークに IP アドレス 209.165.201.29 が含まれています。このアドレスはインターネット上にあり、example.com に属しています。内部のクライアントが example.com にアクセスしても、パケットは FWSM に到達しません。これは、クライアントが 209.165.201.29 がローカルの内部ネットワーク上にあると判断するためです。

この動作を修正するには、**alias** コマンドを次のように使用します。

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

次の例では、Web サーバが内部の 10.1.1.11 にあり、このサーバ用に作成した **static** コマンド文では 209.165.201.11 を指定しています。発信元ホストは、外部のアドレス 209.165.201.7 にあります。外部の DNS サーバには、次に示すとおり、www.example.com のレコードが登録されています。

```
dns-server# www.example.com. IN A 209.165.201.11
```

ドメイン名 www.example.com. の末尾のピリオドは必要です。

次に、**alias** コマンドの使用例を示します。

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

FWSM は、内部クライアント用のネームサーバ応答を 10.1.1.11 に変更して、Web サーバに直接接続できるようにします。

アクセスを可能にするには、次のコマンドも必要です。

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host
209.165.201.11 eq telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成します。
clear configure alias	コンフィギュレーションからすべての **alias** コマンドを削除します。
show running-config alias	オーバーラップするアドレスをデュアル NAT コマンドとともにコンフィギュレーション内に表示します。
static	ローカル IP アドレスをグローバル IP アドレス、あるいはローカル ポートをグローバル ポートにマッピングして、1 対 1 のアドレス変換ルールを設定します。

allocate-acl-partition

メモリ パーティションにコンテキストを割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-acl-partition** コマンドを使用します。割り当てを解除するには、このコマンドの **no** 形式を使用します。

allocate-acl-partition *partition_number*

no allocate-acl-partition *partition_number*

シンタックスの説明

partition_number	パーティション番号を 0 からパーティションの利用可能数から 1 を引いた整数の間で指定します。デフォルトは 12 で、指定できる範囲は 0 ～ 11 です。メモリ パーティションの数を設定する方法については、**resource acl-partition** コマンドを参照してください。

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
コンテキスト コンフィギュレーション	該当なし	該当なし	—	—	•

コマンド履歴

リリース	変更
2.3(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

マルチコンテキスト モードでは、FWSM はルール コンフィギュレーションに割り当てるメモリを分割し、パーティションに各コンテキストを割り当てます。デフォルトで、コンテキストは 12 のパーティションの 1 つに割り当てられます。1 つのパーティションで、ACE、AAA ルールなどを含めて、最大 12,130 のルールを提供します。FWSM は、起動時にロードされた順序で、パーティションにコンテキストを割り当てます。たとえば、12 のコンテキストがある場合、各コンテキストはそれぞれ専用のパーティションに割り当てられ、1 つのコンテキストで 12,130 のルールを使用できます。コンテキストをもう 1 つ追加すると、コンテキスト番号 1 と新しいコンテキスト番号 13 の両方がパーティション 1 に割り当てられ、12,130 のルールを分け合って使用できます。他の 11 のコンテキストは引き続き、それぞれ 12,130 のルールを使用できます。コンテキストを削除しても、パーティションのメンバーシップは変わらないので、リブートしないかぎり、分配が不平等になることがあります。リブートすると、コンテキストが均等に分配されます。

（注） ルールは早いもの順に使用されるので、あるコンテキストが別のコンテキストより多くのルールを使用する場合があります。

もう 1 つの方法として、**allocate-acl-partition** コマンドを使用して、手動でコンテキストをパーティションに割り当てることができます。また、**resource acl-partition** コマンドで設定したコンテキスト数により近づくように、パーティション数減らすことができます。

コンテキストをパーティションに割り当てると、パーティションが*排他的*になります。排他的なパーティションには、そのパーティションに明確に割り当てたコンテキストだけが含まれます。明確に割り当てられたコンテキストがないパーティションは包括的で、ラウンド ロビン方法でコンテキストが割り当てられます。

（注） すべてのパーティションにコンテキストを割り当てた場合、すべてが排他的になります。ただし、パーティションに割り当てられていないコンテキストをあとで追加する場合は、デフォルトでパーティション 0 に割り当てられます。

例

次に、パーティション 0 にコンテキスト test を割り当てる例を示します。

```
hostname# context test
hostname(config-ctx)# allocate-acl-partition 0
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを設定します。
resource acl-partition	マルチ コンテキスト モードのメモリ パーティション数を判別します。
show resource acl-partition	各メモリ パーティションに割り当てられているコンテキストおよび使用されているルール数を表示します。

allocate-interface

セキュリティ コンテキストにインターフェイスを割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。コンテキストからインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

allocate-interface vlan*number*[**-vlan***number*] [*map_name*[**-***map_name*]] [***visible*** | ***invisible***]

no allocate-interface vlan*number*[**-vlan***number*]

シンタックスの説明

invisible	（デフォルト）コンテキスト ユーザに対して、**show interface** コマンドのマッピング名（設定されている場合）だけを表示します。

map_name	（任意）マッピング名を設定します。
	
	map_name は、VLAN ID の代わりに、コンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しないと、コンテキスト内で VLAN ID が使用されます。セキュリティ保護のため、コンテキストの管理者にコンテキストが使用するインターフェイスを知らせたくない場合があります。
	
	マッピング名は文字で開始し、文字または数字で終了する必要があります。中間の文字に使用できるのは、文字、数字、またはアンダースコアだけです。たとえば、次の名前を使用できます。
	
	`int0`
	
	`inta`
	
	`int_0`
	
	マッピング名の範囲を指定できます。範囲に関する詳細については、「使用上のガイドライン」を参照してください。

visible	（任意）マッピング名が設定されている場合でも、コンテキスト ユーザに対して **show interface** コマンドの物理インターフェイスのプロパティを表示します。
vlan*number*	VLAN 番号（通常、2 ～ 1000、1025 ～ 4094）を設定します（サポートされている VLAN のスイッチ マニュアルを参照してください）。FWSM で現在設定されているすべてのインターフェイスを表示するには、**show running-config interface** コマンドまたは **show interface** コマンドを入力します。システムのコンフィギュレーションに存在するインターフェイスだけを割り当てることができます。デフォルトでは、スイッチが FWSM に割り当てるすべての VLAN がシステムのコンフィギュレーションに追加されます。手動で VLAN をシステムのコンフィギュレーションに追加することもできますが、トラフィックを流すためには、スイッチから割り当てる必要があります。

デフォルト

マッピング名を設定した場合、デフォルトで **show interface** コマンドの出力に VLAN ID は表示されません。

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
コンテキスト コンフィギュレーション	該当なし	該当なし	—	—	•

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

異なる範囲を指定するのに、このコマンドを 2 回以上入力できます。マッピング名または参照できる設定を変更するには、所定の VLAN ID のコマンドを再入力して、新しい値を設定します。**no allocate-interface** コマンドを入力して、もう一度やり直す必要はありません。**allocate-interface** コマンドを削除する場合、FWSM によってコンテキスト内のインターフェイスに関連したコンフィギュレーションがすべて削除されます。

必要な場合、ルーテッド モードの複数のコンテキストに同じインターフェイスを割り当てることができます。トランスペアレント モードでは、共有インターフェイスを使用できません。

VLAN ID の範囲を指定する場合には、マッピング名の一致範囲を指定できます。次の範囲に関する注意事項に従ってください。

- マッピング名では、英字部分に続けて数字部分を記述する必要があります。範囲の両端を示すマッピング名の英字部分は、一致している必要があります。たとえば、次の範囲を入力します。

  int0-int10

- マッピング名の数字部分には、**vlan***x*-**vlan***y* ステートメントと同じ数の数字を指定する必要があります。次の例では、両方の範囲に 100 のインターフェイスが含まれています。

  vlan100-vlan199 int1-int100

  たとえば、**vlan100-vlan199 int1-int15** または **vlan100-vlan199 happy1-sad5** と入力すると、コマンドは有効になりません。

例

次に、コンテキストに割り当てられた 100、200、および 300 ～ 305 の VLAN の例を示します。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan200 int2
hostname(config-ctx)# allocate-interface vlan300-vlan305 int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーション内にセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
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。
show context	コンテキスト（システム実行スペース）リストまたは現在のコンテキストに関する情報を表示します。
show interface	インターフェイスのランタイム ステータスおよび統計情報を表示します。

area

OSPF エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*

no area *area_id*

シンタックスの説明

area_id	作成するエリアの ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 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
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

作成するエリアには、パラメータが設定されていません。エリア パラメータを設定するには、関連するエリア コマンドを使用します。

例

次に、エリア ID 1 を使用して、OSPF エリアを作成する例を示します。

```
hostname(config-router)# area 1
hostname(config-router)#
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
area nssa	エリアを NSSA として定義します。
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area authentication

OSPF エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。エリアの認証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。

area *area_id* **authentication** [***message-digest***]

no area *area_id* **authentication** [***message-digest***]

シンタックスの説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
message-digest	（任意）*area_id* で指定されるエリアの Message Digest 5（MD5）認証をイネーブルにします。

デフォルト

エリアの認証は、ディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

指定した OSPF エリアが存在しない場合は、コマンドが入力されるときに作成されます。***message-digest*** キーワードを指定せずに **area authentication** コマンドを入力すると、単純なパスワードの認証がイネーブルになります。***message-digest*** キーワードを指定すると、MD5 認証がイネーブルになります。

例

次に、エリア 1 の MD5 認証をイネーブルにする例を示します。

```
hostname(config-router)# area 1 authentication message-digest
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area default-cost

スタブまたは Not-So-Stubby-Area（NSSA）に送信されるデフォルト サマリー ルートのコストを指定するには、ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* ***default-cost*** *cost*

no area *area_id* ***default-cost***

シンタックスの説明

area_id	デフォルトのコストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
cost	スタブまたは NSSA で使用するデフォルト サマリー ルートのコストを指定します。有効値は 0 ～ 65535 です。

デフォルト

cost のデフォルト値は 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
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

指定したエリアが **area** コマンドで定義されていない場合、このコマンドは指定したパラメータを使用してエリアを作成します。

例

次に、スタブまたは NSSA に送信されるサマリー ルートのデフォルト コストを指定する例を示します。

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
area nssa	エリアを NSSA として定義します。
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area filter-list prefix

ABR の OSPF エリア間のタイプ 3 LSA でアドバタイズされたプレフィクスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list** ***prefix*** *list_name* {***in*** | ***out***}

no area *area_id* ***filter-list prefix*** *list_name* {***in*** | ***out***}

シンタックスの説明

area_id	フィルタリングを設定するエリアの ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
in	指定エリアに着信するアドバタイズされたプレフィクスに、設定済みプレフィクス リストを適用します。
list_name	プレフィクス リストの名前を指定します。
out	指定エリアから発信されるアドバタイズされたプレフィクスに、設定済みプレフィクス リストを適用します。

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
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

指定したエリアが **area** コマンドで定義されていない場合、このコマンドは指定したパラメータを使用してエリアを作成します。

フィルタリングできるのは、タイプ 3 の LSA だけです。ASBR がプライベート ネットワークに設定されている場合、プライベート ネットワークを記述するタイプ 5 の LSA を送信し、その LSA は公共エリアを含むすべての AS にフラッディングされます。

例

次に、他のエリアすべてからエリア 1 に送信されるプレフィクスをフィルタリングする例を示します。

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area nssa

エリアを Not-So-Stubby-Area（NSSA）として設定するには、ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。エリアから NSSA の指定を解除するには、このコマンドの **no** 形式を使用します。

area *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

no area *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

シンタックスの説明

area_id	NSSA として指定するエリアの ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR または NSSA ASBR でのみ有効です。
metric *metric_value*	（任意）OSPF のデフォルト メトリック値を指定します。有効値は 0 ～ 16777214 です。
metric-type {***1*** | ***2***}	（任意）デフォルト ルートの OSPF メトリック タイプ。有効値は、次のとおりです。 • ***1*** — タイプ 1 • ***2*** — タイプ 2 デフォルト値は 2 です。
no-redistribution	（任意）ルータが NSSA ABR の場合に、**redistribute** コマンドを使用して NSSA エリアではなく、通常エリアだけにルートをインポートするときに使用します。
no-summary	（任意）エリアを NSSA とし、サマリー ルートがインポートされないようにします。

デフォルト

デフォルトの設定は次のとおりです。

- NSSA エリアは定義されていません。
- ***metric-type*** は 2 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

指定したエリアが **area** コマンドで定義されていない場合、このコマンドは指定したパラメータを使用してエリアを作成します。

エリアに 1 つのオプションを設定し、あとで別のオプションを指定する場合、両方のオプションが設定されます。たとえば、別々に次の 2 つのコマンドを入力すると、両方のオプションによる 1 つのコマンドがコンフィギュレーションに設定されます。

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

例

次に、2 つのオプションを別々に入力し、コンフィギュレーションに 1 つのコマンドを設定する例を示します。

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area range

エリアの境界でルートを統合し、集約するには、ルータ コンフィギュレーション モードで **area range** 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。

area *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

no area *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

シンタックスの説明

address	サブネット範囲の IP アドレス
advertise	（任意）アドレス範囲ステータスを advertise に設定し、タイプ 3 の集約 Link-State Advertisement（LSA; リンク ステート アドバタイズ）を生成します。
area_id	範囲を設定するエリアの ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク
not-advertise	（任意）アドレス範囲ステータスを DoNotAdvertise に設定します。タイプ 3 の集約 LSA は抑制されていて、コンポーネント ネットワークは他のネットワークから隠されたままです。

デフォルト

アドレス範囲のステータスは、advertise に設定されています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

指定したエリアが **area** コマンドで定義されていない場合、このコマンドは指定したパラメータを使用してエリアを作成します。

area range コマンドは、ABR でのみ使用されます。このコマンドは、エリアのルートを統合または集約する場合に使用されます。このコマンドを使用すると、ABR は 1 つのサマリー ルートを他のエリアにアドバタイズします。エリアの境界で、ルーティング情報が集約されます。エリア外では、1 つのルートが各アドレス範囲にアドバタイズされます。この動作は、*経路集約*と呼ばれます。1 つのエリアに対して、複数の **area range** コマンドを設定できます。このようにして OSPF は、多種多様なアドレス範囲のセットのアドレスを集約します。

no area *area_id* **range** *ip_address netmask* ***not-advertise*** コマンドは、***not-advertise*** オプション キーワードだけを削除します。

例

次に、ABR が 1 つのサマリー ルートを他のエリア（ネットワーク 10.0.0.0 の全サブネットおよびネットワーク 192.168.110.0 の全ホストのエリア）にアドバタイズするように指定する例を示します。

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリアの機能を削除するには、このコマンドの **no** 形式を使用します。

area *area_id* [***no-summary***]

no area *area_id* [***no-summary***]

シンタックスの説明

area_id	スタブ エリアの ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
no-summary	ABR が集約リンク アドバタイズをスタブ エリアに送信しないようにします。

デフォルト

デフォルトの動作は、次のとおりです。

- スタブ エリアは、定義されていません。
- 集約リンク アドバタイズは、スタブ エリアに送信されます。

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
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

このコマンドは、スタブまたは Not-So-Stubby-Area（NSSA）に付属する ABR にのみ使用できます。

area stub コマンドと **area default-cost** コマンドの 2 つのスタブ エリア ルータ コンフィギュレーション コマンドがあります。スタブ エリアに付属するすべてのルータおよびアクセス サーバでは、**area stub** コマンドを使用して、エリアがスタブ エリアとして設定されている必要があります。**area default-cost** コマンドは、スタブ エリアに付属する ABR でのみ使用します。**area default-cost** コマンドは、ABR が生成したサマリー デフォルト ルートのメトリックをスタブ エリアに提供します。

例

次に、指定したエリアをスタブ エリアとして設定する例を示します。

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定します。
area nssa	エリアを NSSA として定義します。
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 running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

area virtual-link

OSPF 仮想リンクを定義するには、ルータ コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットしたり、仮想リンクを削除したりするには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

no area *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

シンタックスの説明

area_id	仮想リンクに対する中継エリアのエリア ID。10 進数または IP アドレスで ID を指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。
authentication	（任意）認証タイプを指定します。
authentication-key *key*	（任意）近接するルーティング デバイスで使用する OSPF 認証パスワードを指定します。
dead-interval *seconds*	（任意）近接するルーティング デバイスがダウンしていることを宣言するまでの Hello メッセージの待機時間を設定します。有効値は 1 ～ 65535 秒です。
hello-interval *seconds*	（任意）インターフェイス上で送信される Hello パケットの間隔を指定します。有効値は 1 ～ 65535 秒です。
md5 *key*	（任意）最大 16 バイトの英数字キーを指定します。
message-digest	（任意）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（任意）Message Digest 5（MD5）認証をイネーブルにし、認証鍵 ID 番号を指定します。有効値は 1 ～ 255 です。
null	（任意）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証が OSPF エリアに設定されていても、無効になります。
retransmit-interval *seconds*	（任意）インターフェイスに属する隣接ルータの LSA 再送信の間隔を指定します。有効値は 1 ～ 65535 秒です。
router_id	仮想リンクのネイバーに関連付けられたルータ ID。ルータ ID は各ルータが、インターフェイスの IP アドレスから内部的に取得します。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（任意）OSPF がトポロジ変更を受信してから、Shortest Path First（SPF）の計算を開始するまでの遅延時間（0 ～ 65535 秒）を指定します。デフォルトは 5 秒です。

デフォルト

デフォルトの設定は次のとおりです。

- *area_id*：エリア ID は事前定義されていません。
- *router_id*：ルータ ID は事前定義されていません。
- ***hello-interval*** *seconds*：デフォルトの値は、10 秒です。
- ***retransmit-interval*** *seconds*：デフォルトの値は、5 秒です。
- ***transmit-delay*** *seconds*：1 秒
- ***dead-interval*** *seconds*：デフォルトの値は、40 秒です。

- ***authentication-key*** *key*：鍵は事前定義されていません。
- ***message-digest-key*** *key_id* ***md5*** *key*：鍵は事前定義されていません。

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
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 では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失敗した場合は、仮想リンクを確立して修正できます。

Hello 間隔が小さいほど、トポロジの変更は短時間で検出されますが、ルーティング トラフィック量が増大します。

不要な再送信が発生しないように、再送信間隔を慎重に設定する必要があります。シリアル回線または仮想リンクには、値を大きくしてください。

送信遅延の値には、インターフェイスの送信遅延と伝播遅延が考慮されている必要があります。

指定した認証鍵は、***area*** *area_id* ***authentication*** コマンドでバックボーンの認証をイネーブルにしている場合にだけ使用できます。

2 つの認証方式である、単純なテキスト認証と MD5 認証は、相互に排他的です。どちらも指定しないか、どちらか一方を指定することが可能です。***authentication-key*** *key* または ***message-digest-key*** *key_id* ***md5*** *key* のあとに指定したキーワードと引数は、無視されます。したがって、このようなキーワードと引数の組み合わせの前にオプションの引数を指定してください。

インターフェイスに認証タイプが指定されていない場合、インターフェイスはエリアに指定されている認証タイプを使用します。エリアに認証タイプが指定されていない場合、エリアのデフォルトはヌル認証になります。

（注） 各仮想リンクのネイバーには、中継エリアの ID が含まれ、仮想リンクの対応する仮想リンク近接ルータ ID が正確に設定されている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

仮想リンク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。仮想リンクを削除するには、**no area** *area_id* ***virtual-link*** コマンドを使用します。

例

次に、MD5 認証を使用して、仮想リンクを確立する例を示します。

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
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	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。
show running-config router	グローバル ルータ コンフィギュレーションに指定されているコマンドを表示します。

arp

ARP テーブルにスタティック ARP エントリを追加するには、グローバル コンフィギュレーション モードで **arp** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。スタティック ARP エントリは、MAC アドレスを IP アドレスにマッピングし、ホストが経由して到達したインターフェイスを特定します。スタティック ARP エントリはタイムアウトしないので、ネットワーク問題を解決するのに役立つ場合があります。トランスペアレント ファイアウォール モードでは、スタティック ARP テーブルが ARP 検査で使用されます（**arp-inspection** コマンドを参照）。

arp *interface_name ip_address mac_address* [***alias***]

no arp *interface_name ip_address mac_address*

シンタックスの説明

alias	（任意）このマッピングのプロキシ ARP をイネーブルにします。FWSM が指定した IP アドレスの ARP 要求を受信すると、FWSM の MAC アドレスを使用して応答します。FWSM が IP アドレスに属するホスト宛てのトラフィックを受信すると、FWSM は、このコマンドで指定するホストの MAC アドレスにトラフィックを転送します。このキーワードは、たとえば、ARP を実行しないデバイスがある場合に役立ちます。 トランスペアレント ファイアウォール モードでは、このキーワードが無視されます。FWSM は、プロキシ ARP を実行しません。
interface_name	ホストのネットワークに接続されたインターフェイス
ip_address	ホストの IP アドレス
mac_address	ホストの MAC アドレス

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

ホストは IP アドレスでパケットの宛先を特定しますが、イーサネット上の実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストが直接接続されたネットワークでパケットを配信する場合、IP アドレスに関連付けられた MAC アドレスを問い合わせる ARP 要求を送信して、その ARP 応答による MAC アドレスにパケットを配信します。ホストまたはルータは ARP テーブルを保持するので、配信するすべてのパケットに対して ARP 要求を送信する必要はありません。ARP 応答がネットワーク上に送信されるときは常に ARP テーブルが動的に更新され、エントリが一定期間使用されなかった場合は、タイムアウトします。エントリが正しくない場合（たとえば、MAC アドレスが所定の IP アドレスに変わる場合）、更新される前にエントリがタイムアウトします。

（注） トランスペアレント ファイアウォール モードでは、管理トラフィックなど FWSM を行き来するトラフィックにダイナミック ARP エントリが使用されます。

例

次に、MAC アドレス 0009.7cbe.2100 を持つ外部インターフェイスに 10.1.1.1 のスタティック ARP エントリを作成する例を示します。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	FWSM が ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	トランスペアレント ファイアウォール モードの場合に、ARP スプーフィングを防止するために ARP パケットを検査します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在の設定を表示します。

arp timeout

FWSM が ARP テーブルを再構築するまでの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 **arp timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。ARP テーブルの再構築では、新しいホスト情報が自動的に更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変わるので、タイムアウト値を小さくする必要がある場合があります。

arp *timeout* *seconds*

no arp *timeout* *seconds*

シンタックスの説明

seconds	ARP テーブルを再構築する秒単位の間隔（60 〜 4294967）

デフォルト

デフォルト値は、14,400 秒（4 時間）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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、ARP タイムアウトを 5000 秒に変更する例を示します。

```
hostname(config)# arp timeout 5000
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードの場合に、ARP スプーフィングを防止するために ARP パケットを検査します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	ARP タイムアウトの現在の設定を表示します。

arp-inspection

トランスペアレント ファイアウォール モードの ARP 検査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 **arp-inspection** コマンドを使用します。ARP 検査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。ARP 検査は、スタティック ARP エントリに対してすべての ARP パケットを比較し（**arp** コマンドを参照）、一致しなかったパケットをブロックします。この機能は、ARP スプーフィングを防止します。

arp-inspection *interface_name* ***enable*** [***flood*** | ***no-flood***]

no arp-inspection *interface_name* ***enable***

シンタックスの説明

enable	ARP 検査をイネーブルにします。
flood	（デフォルト）スタティック ARP エントリの要素に一致しないパケットが、発信元インターフェイス以外のすべてのインターフェイスにフラッディングされるように指定します。MAC アドレス、IP アドレス、またはインターフェイス間で不一致が生じすると、FWSM はパケットを廃棄します。
interface_name	ARP 検査をイネーブルにするインターフェイス
no-flood	（任意）スタティック ARP エントリに完全に一致しないパケットを廃棄するように指定します。

デフォルト

デフォルトでは、すべてのインターフェイスで ARP 検査がディセーブルにされています。すべての ARP パケットは、FWSM を通過できます。ARP 検査をイネーブルにすると、デフォルトが、一致しない ARP パケットをフラッディングさせる動作になります。

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
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

ARP 検査をイネーブルにする前に、**arp** コマンドを使用して、スタティック ARP エントリを設定します。

ARP 検査をイネーブルにすると、FWSM は、すべての ARP パケットの MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブルのスタティック エントリと比較して、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリに一致した場合、パケットが通過します。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致が生じすると、FWSM はパケットを廃棄します。

- スタティック ARP テーブルのエントリに ARP パケットが一致しない場合は、FWSM がすべてのインターフェイスにパケットを転送（フラッディング）するか、パケットを廃棄するかを設定できます。

ARP 検査は、悪意のあるユーザが他のホストまたはルータになりすますのを防ぎます（別名、ARP スプーフィング）。ARP スプーフィングは、[man-in-the-middle] 攻撃を可能にします。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信するとします。ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスを返しますが、攻撃者は、ルータの MAC アドレスではなく、攻撃者の MAC アドレスでホストに別の ARP 応答を送信します。これにより、攻撃者は、すべてのホスト トラフィックを傍受してから、ルータに転送することが可能になります。

正しい MAC アドレスと関連付けられた IP アドレスがスタティック ARP テーブルに存在する間は、ARP 検査により、攻撃者は攻撃者の MAC アドレスを使用して ARP 応答を送信することはできません。

（注） トランスペアレント ファイアウォール モードでは、管理トラフィックなど FWSM を行き来するトラフィックにダイナミック ARP エントリが使用されます。

例

次に、外部インターフェイスの ARP 検査をイネーブルにして、スタティック ARP エントリに一致しない ARP パケットを廃棄するように FWSM を設定する例を示します。

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
clear configure arp-inspection	ARP 検査の設定を消去します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在の設定を表示します。

asdm disconnect

アクティブ ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

シンタックスの説明

session	終了するアクティブ ASDM セッションのセッション ID。**show asdm sessions** コマンドを使用して、すべてのアクティブ ASDM セッションのセッション ID を表示できます。

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)	**pdm disconnect** コマンドとして、このコマンドが追加されました。
3.1(1)	このコマンドが **pdm disconnect** コマンドから **asdm disconnect** コマンドに変更されました。

使用上のガイドライン

アクティブ ASDM セッションと対応付けられたセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ある ASDM セッションを終了しても、残りのアクティブな ASDM セッションは、それぞれのセッション ID と関連付けられたままです。たとえば、0、1、2 のセッション ID を持つ 3 つのアクティブ ASDM セッションが存在する場合、セッション 1 を終了しても、残りのアクティブ ASDM セッションは 0 と 2 のセッション ID を保持したままです。このとき、次の新規 ASDM セッションには、セッション ID として 1 が割り当てられ、以降の新規セッションは、セッション ID 3 から始まります。

例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**show asdm sessions** コマンドは、**asdm disconnect** コマンドが入力された前後のアクティブ ASDM セッションを表示します。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブ ASDM セッションと対応付けられたセッション ID のリストを表示します。

asdm disconnect log_session

アクティブ ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

asdm disconnect log_session *session*

シンタックスの説明

session	終了するアクティブ ASDM ロギング セッションのセッション ID。**show asdm log_sessions** コマンドを使用して、すべてのアクティブ ASDM セッションのセッション ID を表示できます。

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
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

アクティブ ASDM ロギング セッションと対応付けられたセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

各アクティブ ASDM セッションには、対応付けられた ASDM ロギング セッションが 1 つまたは複数あります。ASDM は、ロギング セッションを使用して、FWSM から Syslog メッセージを取得します。ログ セッションを終了すると、アクティブ ASDM セッションに悪影響を与える可能性があります。不要な ASDM セッションと対応付けられたログ セッションを終了するには、**asdm disconnect** コマンドを使用します。

（注） 各 ASDM セッションには最低 1 つの ASDM ロギング セッションがあるので、**show asdm sessions** と **show asdm log_sessions** の出力が同じになる場合があります。

ある ASDM ロギング セッションを終了しても、残りのアクティブな ASDM ロギング セッションは、それぞれのセッション ID と関連付けられたままです。たとえば、0、1、2 のセッション ID を持つ 3 つのアクティブ ASDM ロギング セッションが存在する場合、セッション 1 を終了しても、残りのアクティブ ASDM ロギング セッションは 0 と 2 のセッション ID を保持したままです。このとき、次の新規 ASDM ロギング セッションには、セッション ID として 1 が割り当てられ、以降の新規ロギング セッションは、セッション ID 3 から始まります。

例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**show asdm log_sessions** コマンドは、**asdm disconnect log_sessions** コマンドが入力された前後のアクティブ ASDM セッションを表示します。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブ ASDM ロギング セッションと対応付けられたセッション ID のリストを表示します。

asdm group

注意　このコマンドは、手動で設定しないでください。ASDM は、**asdm group** コマンドを実行コンフィギュレーションに追加して、内部用途で使用します。このコマンドの説明は、情報として提供することを目的としてこのマニュアルに含まれています。

asdm group *real_grp_name real_if_name*

asdm group *ref_grp_name ref_if_name* ***reference*** *real_grp_name*

シンタックスの説明

real_grp_name	ADSM オブジェクト グループの名前
real_if_name	指定されたオブジェクト グループが関連付けられているインターフェイスの名前
ref_grp_name	*real_grp_name* 引数で指定されたオブジェクト グループの変換 IP アドレスを含むオブジェクト グループの名前
ref_if_name	インバウンド トラフィックの宛先 IP アドレスの変換元になるインターフェイスの名前

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
1.1(1)	**pdm group** コマンドとして、このコマンドが追加されました。
3.1(1)	このコマンドが **pdm group** コマンドから **asdm group** コマンドに変更されました。

使用上のガイドライン

このコマンドは、手動で設定したり、削除したりしないでください。

asdm history enable

ASDM 履歴トラッキング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 **asdm history enable** コマンドを使用します。ASDM 履歴トラッキング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。

asdm history enable

no asdm history 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

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)	**pdm history enable** コマンドとして、このコマンドが追加されました。
3.1(1)	このコマンドが **pdm history enable** コマンドから **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにしたことによって得られた情報は、ASDM 履歴バッファに保存されます。**show asdm history** コマンドを使用して、この情報を表示できます。ASDM は、デバイスのモニタリングで履歴情報を使用します。

例

次に、ASDM 履歴トラッキングをイネーブルにする例を示します。

```
hostname(config)# asdm history enable
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm location

注意　このコマンドは、手動で設定しないでください。ASDM は、**asdm location** コマンドを実行コンフィギュレーションに追加して、内部通信で使用します。このコマンドの説明は、情報として提供することを目的としてこのマニュアルに含まれています。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

シンタックスの説明

ip_addr	ネットワーク トポロジを定義するために ASDM が内部で使用する IP アドレス
netmask	*ip_addr* のサブネット マスク
if_name	ASDM にアクセスするためのインターフェイスの名前
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM が内部で使用する IPv6 アドレスとプレフィクス

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)	**pdm location** コマンドとして、このコマンドが追加されました。
3.1(1)	このコマンドが **pdm location** コマンドから **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドは、手動で設定したり、削除したりしないでください。

asr-group

非対称ルーティング インターフェイスのグループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

asr-group *group_id*

no asr-group *group_id*

シンタックスの説明

group_id	非対称ルーティングのグループ ID。有効値は、1 ～ 32 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
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
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

場合によっては、セッションのリターン トラフィックが送信元とは別のインターフェイスでルーティングされることがあります。フェールオーバー構成では、1 台の装置から発信された接続のリターン トラフィックが、ピア装置を介して戻される場合があります。これは通常、1 台の FWSM またはフェールオーバー ペア構成の 2 台の FWSM にある 2 つのインターフェイスが異なるサービス プロバイダーに接続されており、アウトバウンド接続が NAT アドレスを使用しない場合に発生します。デフォルトでは、トラフィックの接続情報がないため、FWSM がリターン トラフィックを廃棄します。

このようなことが発生しやすいインターフェイスに対して **asr-group** コマンドを使用して、リターン トラフィックの廃棄を防ぐことができます。**asr-group** コマンドで設定したインターフェイスが、セッション情報を持たないパケットを受信すると、同じグループに存在する他のインターフェイスのセッション情報を確認します。

（注） フェールオーバー構成では、スタンバイ装置またはフェールオーバー　グループからアクティブ装置またはフェールオーバー グループに渡すセッション情報のステートフル フェールオーバーをイネーブルにする必要があります。

一致しない場合は、パケットが廃棄されます。一致する場合は、次のいずれかのアクションが実行されます。

- 着信トラフィックがフェールオーバー構成のピア装置から発信されている場合、レイヤ 2 のヘッダーの一部またはすべてが書き換えられ、相手装置にパケットがリダイレクトされます。このリダイレクションは、セッションがアクティブな間、継続します。
- 着信トラフィックが同じ装置の異なるインターフェイスから発信されている場合、レイヤ 2 のヘッダーの一部またはすべてが書き換えられ、ストリームにパケットが再挿入されます。

（注）　非対称ルーティングのサポートを設定するのに **asr-group** コマンドを使用すると、***nailed*** オプションを指定して **static** コマンドを使用する場合より、セキュリティが高くなります。

show interface detail コマンドを使用して、ASR の統計情報を表示できます。これらの統計情報には、インターフェイスに送信された ASR パケット数、インターフェイスで受信された ASR パケット数、およびインターフェイスで廃棄された ASR パケット数が含まれます。

例

次に、選択したインターフェイスを非対称ルーティングのグループ 1 に割り当てる例を示します。

コンテキスト ctx1 のコンフィギュレーションは、次のとおりです。

```
hostname/ctx1(config)# interface Vlan101
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーションは、次のとおりです。

```
hostname/ctx2(config)# interface Vlan102
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

関連コマンド

コマンド	説明
interface	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。
show interface	インターフェイスの統計情報を表示します。

authentication-port

このホストの RADIUS 認証で使用されるポート番号を指定するには、AAA サーバ ホスト モードで **authentication-port** コマンドを使用します。認証ポートの指定を解除するには、このコマンドの **no** 形式を使用します。このコマンドは、認証機能の割り当て先となるリモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。

authentication-port *port*

no authentication-port

シンタックスの説明

port	RADIUS 認証のポート番号（1 ～ 65535 の範囲）

デフォルト

デフォルトでは、デバイスはポート 1645（RFC 2058 に準拠）で RADIUS を待ち受けます。ポートが指定されないと、RADIUS 認証のデフォルト ポート番号（1645）が使用されます。

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
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更
3.1(1)	**aaa-server radius-authport** コマンドに代わって、このコマンドが追加されました。

使用上のガイドライン

RADIUS 認証サーバが 1645 以外のポートを使用している場合、**aaa-server** コマンドで RADIUS サービスを起動する前に、FWSM に適切なポートを設定する必要があります。

ヒント　RFC 2138 によって、RADIUS 認証の標準ポートがポート 1812 に変更されました。

このコマンドは、RADIUS 用に設定されているサーバ グループでのみ有効です。

例

次に、ホスト [1.2.3.4] の [svrgrp1] という名前の RADIUS AAA サーバを設定する例を示します。タイムアウトを 9 秒、再試行間隔を 7 秒に設定し、認証ポート 1650 を設定します。

```
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 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上の LOCAL、TACACS+、または RADIUS ユーザ認証のほか、ASDM ユーザ認証をイネーブルまたはディセーブルにします。
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 サーバの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-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について、AAA サーバの統計情報を表示します。

authentication-server-group

ユーザ認証で使用する AAA サーバ グループを指定するには、tunnel-group general-attributes モードで **authentication-server-group** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの ***no*** 形式を使用します。

authentication-server-group [(*interface name*)] *server group* [***LOCAL*** | ***NONE***]

no authentication-server-group [(*interface name*)] *server group*

シンタックスの説明

interface name	（任意）IPSec トンネルが終端するインターフェイスを指定します。
LOCAL	（任意）サーバ グループのすべてのサーバが通信障害によって無効にされている場合に、ローカル ユーザ データベースに対して実行する認証を指定します。サーバ グループ名が ***LOCAL*** または ***NONE*** *の場合*、ここで ***LOCAL*** キーワードを使用しないでください。
NONE	（任意）サーバ グループ名がないことを指定します。認証が不要であることを指定するには、***NONE*** キーワードをサーバ グループ名として使用します。
server group	AAA サーバ グループの名前を指定します。デフォルトは、***LOCAL*** です。

デフォルト

このコマンドのデフォルト設定は、***LOCAL*** 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

この属性は、IPSec リモート アクセス トンネル グループ タイプにのみ適用できます。

例

次に、config-general コンフィギュレーション モードで、remotegrp という名前の IPSec リモート アクセス トンネル グループに対して、aaa-server456 という名前の認証サーバ グループを設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバのパラメータを設定します。
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 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。

authorization-dn-attributes

許可用のユーザ名にサブジェクト DN フィールドのどの部分を使用するかを指定するには、tunnel-group ipsec-attributes コンフィギュレーション モードで **authorization-dn-attributes** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの ***no*** 形式を使用します。

[no] authorization-dn-attributes {*primary-attr* [*secondary-attr*] | ***use-entire-name***}

シンタックスの説明

primary-attr	証明書から許可クエリーの名前を抽出するのに使用する属性を指定します。
secondary-attr	（任意）プライマリ属性が存在しない場合に、証明書から許可クエリーの名前を抽出するのに使用する追加の属性を指定します。
use-entire-name	FWSM が名前を抽出するのにすべてのサブジェクト DN（RFC 1779）を使用するように指定します。

デフォルト

プライマリ属性のデフォルト値は、CN（一般名称）です。

セカンダリ属性のデフォルト値は、OU（組織ユニット）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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　この属性は、IPSec リモート アクセス トンネル タイプにのみ適用できます。

プライマリおよびセカンダリ属性の内容は、次のとおりです。

属性	定義
CN	Common Name（一般名称）：個人、システム、または他のエンティティの名前
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ
O	Organization（組織）：企業、機関、代理店、アソシエーション、または他のエンティティの名前
L	Locality（地名）：組織が所在する市区町村
SP	State/Province（都道府県 / 地域）：組織が所在する都道府県や地域
C	Country（国）：2 文字の国名省略語。これらのコードは、ISO 3166 国名省略語に準拠しています。
EA	E-mail Address（電子メール アドレス）
T	Title（タイトル）
N	Name
GN	Given Name（ファーストネーム）
SN	Surname（名字）
I	Initials（イニシャル）
GENQ	Generational Qualifier（一般的な修飾子）
DNQ	Domain Name Qualifier（ドメイン名修飾子）
UID	User Identifier（ユーザ識別子）

例　次に、config-ipsec コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループ（ipsec_ra）を作成し、IPSec グループ属性を指定し、許可用のユーザ名に一般名称を使用するように定義する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# authorization-dn-attributes CN
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。
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-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。

authorization-required

許可が行われ、ユーザがサーバに正常に接続できるようにするには、tunnel-group ipsec-attributes コンフィギュレーション モードで **authorization-required** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの ***no*** 形式を使用します。

[no] authorization-required

デフォルト

このコマンドのデフォルト設定は、ディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。

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 トンネルグループ タイプだけです。

例

次に、config-ipsec コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループを介して接続するユーザに対してすべての DN に基づく許可を要求する例を示します。最初のコマンドは、ipsec_ra（IPSec リモート アクセス）として remotegrp という名前のリモート グループのトンネル グループ タイプを設定しています。次のコマンドは指定したトンネル グループの ipsec-attributes モードを開始しています。最後のコマンドは名前が付けられたトンネル グループで要求する許可を指定しています。

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

authorization-server-group

ユーザの許可で AAA サーバ グループを指定するには、tunnel-group general-attributes モードで **authorization-server-group** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの ***no*** 形式を使用します。

authorization-server-group *server group*

no authorization-server-group

シンタックスの説明

server group	AAA サーバ グループの名前を指定します。デフォルトは、***none*** です。

デフォルト

このコマンドのデフォルト設定は、***no authorization-server-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
tunnel-group general-attributes	•	•	•	•	—

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

この属性は、IPSec remote-access Tunnel-group タイプのみに適用できます。

VPN Authorization が LOCAL として定義されている場合、デフォルトのグループ ポリシーである DfltGrpPolicy に設定された属性が実装されます。

例

次に、config-general コンフィギュレーション モードで、[remotegrp] という名前の IPSec リモート アクセス トンネル グループに対して、[aaa-server78] という名前の許可サーバ グループを設定する例を示します。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバのパラメータを設定します。
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 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。

auth-prompt

FWSM 経由のユーザ セッションの AAA チャレンジ テキストを指定したり、変更したりするには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキ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。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

シンタックスの説明

accept	Telnet 経由のユーザ認証が許可される場合、プロンプトの *string* を表示します。
prompt	AAA チャレンジ プロンプト文字列がこのキーワードのあとに続きます。
reject	Telnet 経由のユーザ認証が拒否される場合、プロンプトの *string* を表示します。
ストリング	235 文字または 31 単語（どちらか最初に達した方）までの英数字で構成される文字列。特殊文字、スペース、句読文字を使用できます。疑問符を入力するか、**Enter** キーを押すと、文字列が終了します（疑問符は、文字列に表示されます）。

デフォルト

認証プロンプトを指定しない場合、ユーザがログインするときに表示されるプロンプトは、使用しているプロトコルに応じて次の内容が表示されます。

- HTTP を使用してログインするユーザに表示されるプロンプト：`HTTP Authentication`
- FTP を使用してログインするユーザに表示されるプロンプト：`FTP Authentication`
- Telnet を使用してログインするユーザには、プロンプトが表示されません。

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
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

TACACS+ または RADIUS サーバからユーザ認証を受ける必要がある場合、**auth-prompt** コマンドを使用すると、FWSM 経由の HTTP、FTP、および Telnet アクセスに対して AAA チャレンジ テキストを指定できます。このテキストの目的は主に外見上のもので、ユーザがログインするときにユーザに表示されるユーザ名とパスワードの上に表示されます。

ユーザ認証が Telnet から発生する場合は、**accept** オプションと **reject** オプションを使用すると、認証試行が AAA サーバで受け入れられたか拒否されたかに応じて、それぞれ異なるステータス プロンプトを表示できます。

AAA サーバがユーザを認証する場合、FWSM はユーザに対して **auth-prompt accept** テキスト（指定した場合）を表示します。それ以外の場合は、**reject** テキスト（指定した場合）を表示します。HTTP セッションと FTP セッションの認証では、プロンプト時にチャレンジ テキストだけを表示します。**accept** と **reject** テキストは表示されません。

（注）　Microsoft Internet Explorer では、認証プロンプトで 37 文字まで表示されます。Netscape Navigator では、120 文字まで表示されます。Telnet と FTP では、認証プロンプトで 235 文字まで表示されます。

例

次に、認証プロンプトを [Please enter your username and password] の文字列に設定する例を示します。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

コンフィギュレーションにこの文字列を追加すると、ユーザには次のプロンプトが表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザの場合、たとえば、FWSM が認証試行を許可または拒否する場合に、別のメッセージを表示させることもできます。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

次に、正常な認証に対する認証プロンプトを [You are OK] という文字列に設定する例を示します。

```
hostname(config)# auth-prompt accept You are OK.
```

正常に認証されたら、次のメッセージがユーザに対して表示されます。

```
You are OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	以前に指定した認証プロンプト チャレンジ テキスト（存在する場合）を削除し、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-update device-id

Auto Update Server で使用する FWSM デバイスの ID 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 **auto-update device-id** コマンドを使用します。デバイスの ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

シンタックスの説明

hardware-serial	FWSM のハードウェア シリアル番号を使用して、デバイスを一意に識別します。
hostname	FWSM のホスト名を使用して、デバイスを一意に識別します。
ipaddress [*if_name*]	FWSM の IP アドレスを使用して、FWSM を一意に識別します。デフォルトでは、Auto Update Server との通信に使用されるインターフェイスを FWSM が使用します。別の IP アドレスを使用する場合は、*if_name* を指定します。
mac-address [*if_name*]	FWSM の MAC アドレスを使用して、FWSM を一意に識別します。デフォルトでは、Auto Update Server との通信に使用される MAC アドレスを FWSM が使用します。別の MAC アドレスを使用する場合は、*if_name* を指定します。
string *text*	Auto Update Server に対するデバイスを一意に識別するテキスト文字列を指定します。

デフォルト

デフォルトの ID は hostname 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。

例

次に、デバイスの ID をシリアル番号に設定する例を示します。

```
hostname(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	FWSM が Auto Update Server からの更新をチェックする頻度を設定します。
auto-update server	Auto Update Server を識別します。
auto-update timeout	Auto Update Server がタイムアウト期間アクセスされていない場合に、FWSM を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server の設定を消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update poll-period

FWSM が Auto Update Server からの更新を確認する頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。パラメータをデフォルト値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。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

シンタックスの説明

poll_period	Auto Update Server をポーリングする頻度（分数）を指定します（1 ～ 35791）。デフォルトは 720 分（12 時間）です。
retry_count	最初の試行が失敗した場合、Auto Update Server に再接続する試行回数を指定します。デフォルトの値は、0 です。
retry_period	接続試行間隔を分数で指定します（1 ～ 35791）。デフォルトは 5 分です。

デフォルト

デフォルトのポーリング間隔は 720 分（12 時間）です。

最初の試行が失敗した場合に、Auto Update Server に再接続するデフォルトの試行回数は 0 です。

デフォルトの接続試行間隔は 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
3.1(1)	このコマンドが追加されました。

例

次に、ポーリング間隔を 360 分に、再試行回数を 1 回、再試行間隔を 3 分に設定する例を示します。

```
hostname(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server で使用する FWSM デバイス ID を設定します。
auto-update server	Auto Update Server を識別します。
auto-update timeout	Auto Update Server がタイムアウト期間アクセスされていない場合に、FWSM を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server の設定を消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update server

Auto Update Server 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 **auto-update server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。FWSM は、コンフィギュレーション、OS（オペレーティング システム）、および ASDM の更新を確認するために、Auto Update Server に定期的にアクセスします。

auto-update server *url* [*verify-certificate*]

no auto-update server *url* [*verify-certificate*]

シンタックスの説明

url	次の構文を使用して、Auto Update Server の場所を指定します。 **http**[**s**]**:**[[*user:password@*]*location* [*:port*]] / *pathname*
verify_certificate	Auto Update Server から戻された証明書を確認します。

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

設定できるサーバ数は、1 つだけです。

例

次に、Auto Update Server の URL を設定する例を示します。

```
hostname(config)# auto-update server http://10.1.1.1:1741/
```

関連コマンド

auto-update device-id	Auto Update Server で使用する FWSM デバイス ID を設定します。
auto-update poll-period	FWSM が Auto Update Server からの更新をチェックする頻度を設定します。
auto-update timeout	Auto Update Server がタイムアウト期間アクセスされていない場合に、FWSM を通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server の設定を消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update timeout

Auto Update Server のアクセスに関するタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。Auto Update Server がタイムアウト期間アクセスされていない場合、FWSM は FWSM を通過するすべてのトラフィックを停止します。タイムアウトを設定して、FWSM のイメージとコンフィギュレーションを最新の状態に保ちます。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

auto-update timeout *period*

no auto-update timeout [*period*]

シンタックスの説明

period	タイムアウト期間を分数で指定します（1 ～ 35791）。デフォルト は 0 です。この値は、タイムアウトがないことを示します。タイムアウトを 0 に設定することはできません。タイムアウトを 0 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。

デフォルト

デフォルトのタイムアウトは 0 です。この値は、FWSM がタイムアウトしないように設定します。

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
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

タイムアウトの状態は、システム ログ メッセージ 201008 で報告されます。

例

次に、タイムアウトを 24 時間に設定する例を示します。

```
hostname(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server で使用する FWSM デバイス ID を設定します。
auto-update poll-period	FWSM が Auto Update Server からの更新をチェックする頻度を設定します。
auto-update server	Auto Update Server を識別します。
clear configure auto-update	Auto Update Server の設定を消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。