CHAPTER 13

gateway コマンド～ hw-module module shutdown コマンド

gateway

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **gateway** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

gateway *ip_address* [*group_id*]

シンタックスの説明

gateway	特定のゲートウェイを管理しているコール エージェントのグループを指定します。
ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

gateway コマンドは、特定のゲートウェイを管理しているコール エージェントのグループを指定するために使用します。*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。*group_id* オプションは 0 ～ 4294967295 の数字です。この数字は、ゲートウェイを管理しているコール エージェントの *group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

例

次の例では、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようにし、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようにしています。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。

global

NAT 用のマッピング アドレスのプールを作成するには、グローバル コンフィギュレーション モードで **global** コマンドを使用します。アドレスの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。

global (*mapped_ifc) nat_id* {*mapped_ip*[**-***mapped_ip*] [**netmask** *mask*] | **interface**}

no global (*mapped_ifc) nat_id* {*mapped_ip*[-*mapped_ip*] [**netmask** *mask*] | **interface**}

シンタックスの説明

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。このキーワードを使用するのは、インターフェイス アドレスを使用しようとする場合に、アドレスが DHCP を使用して動的に割り当てられているときです。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip[**-***mapped_ip*]	マッピングされているインターフェイスの終了時に実際のアドレスを変換する場合の変換先マッピング アドレス（複数可）を指定します。単一のアドレスを指定する場合は、PAT を設定します。アドレスの範囲を指定する場合は、ダイナミック NAT を設定します。 外部ネットワークがインターネットに接続されている場合は、各グローバル IP アドレスが Network Information Center（NIC）に登録されている必要があります。
nat_id	NAT ID の整数を指定します。この ID は、変換対象の実際のアドレスにマッピング プールを関連付けるときに **nat** コマンドによって参照されます。 通常の NAT の場合、この整数の範囲は 1 ～ 2147483647 となります。ポリシー NAT（**nat id access-list**）の場合、整数の範囲は 1 ～ 65535 となります。 **global** コマンドで NAT ID に 0 を指定しないでください。0 は、**global** コマンドを使用しないアイデンティティ NAT および NAT 免除用に予約されています。
netmask *mask*	（オプション）*mapped_ip* のネットワーク マスクを指定します。このマスクは、*mapped_ip* と組み合せた場合、ネットワークを指定しません。この場合は、*mapped_ip* をホストに割り当てるときに mapped_ip に割り当てたサブネット マスクを指定します。アドレスの範囲を設定する場合は、*mapped_ip-mapped_ip* を指定する必要があります。 マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	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	
	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ダイナミック NAT および PAT の場合は、最初に、変換対象となるインターフェイス上の実際のアドレスを指定する **nat** コマンドを設定します。次に、別のインターフェイスの終了時にマッピング アドレスを指定するための **global** コマンドを別途設定します（PAT の場合、マッピング アドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、**global** コマンドと一致します。

ダイナミック NAT および PAT の詳細については、**nat** コマンドを参照してください。

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするのを待たずに新しい NAT 情報を使用するときは、**clear xlate** コマンドを使用して変換テーブルを消去してもかまいません。ただし、変換テーブルを消去すると現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
clear configure global	**global** コマンドをコンフィギュレーションから削除します。
nat	変換対象となる実際のアドレスを指定します。
show running-config global	コンフィギュレーション内の **global** コマンドを表示します。
static	1 対 1 の変換を設定します。

group

IKE ポリシーの Diffie-Hellman グループを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子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。

group {**1** | **2** | **5** | **7**}

no group

シンタックスの説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1,536 ビットの Diffie-Hellman グループ 5 が使用されるように指定します。
group 7	IKE ポリシーで、Diffie-Hellman Group 7 を使用することを指定します。Group 7 は IPSec SA キーを生成します。楕円曲線フィールドのサイズは 163 ビットです。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトのグループ ポリシーは、group 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy group** コマンドが導入されました。
7.2.(1)	**isakmp policy group** コマンドが、**group** コマンドに置き換えられました。

使用上のガイドライン

グループ オプションには、768 ビット（DH Group 1）、1,024 ビット（DH Group 2）、1,536 ビット（DH Group 5）、および DH Group 7 の 4 つがあります。1,024 ビットと 1,536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注）　Cisco VPN クライアントのバージョン 3.x 以上では、ISAKMP ポリシーで DH グループ 2 を使用する必要があります（DH グループ 1 に設定すると接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES のキーのサイズは非常に大きいので、ISAKMP ネゴシエーションで Diffie-Hellman（DH）グループ 1 や 2 ではなく、グループ 5 を使用する必要があります。この設定を行うには、**group 5** コマンドを使用します。

例

次の例は、グローバル コンフィギュレーション モードで、**group** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに、グループ 2、1024 ビット Diffie Hellman を使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# group 2
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

group-alias

ユーザがトンネル グループを参照できるように 1 つまたは複数の代替名を作成するには、トンネル グループ webvpn コンフィギュレーション モードで **group-alias** コマンドを使用します。リストからエイリアスを削除するには、このコマンドの **no** 形式を使用します。

group-alias *name* [***enable*** | ***disable]***

no group-alias *name*

シンタックスの説明

disable	グループ エイリアスをディセーブルにします。
enable	以前にディセーブルにしたグループ エイリアスをイネーブルにします。
name	トンネル グループ エイリアスの名前を指定します。名前には、スペースは使用できませんが、それ以外は任意の文字列を選択できます。

デフォルト

デフォルトのグループ エイリアスはありませんが、グループ エイリアスを指定すると、そのエイリアスがデフォルトでイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ここで指定したグループ エイリアスは、ログイン ページのドロップダウン リストに表示されます。各グループはエイリアスを複数持ってもよいし、まったく持たなくてもかまいません。このコマンドは、同じグループが「Devtest」や「QA」などの複数の通常名で知られている場合に有用です。

例

次の例は、「devtest」という名前の webvpn トンネル グループを設定し、そのグループに対してエイリアス「QA」および「Fra-QA」を確立するコマンドを示しています。

```
hostname(config)# tunnel-group devtest type webvpn
hostname(config)# tunnel-group devtest webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias QA
hostname(config-tunnel-webvpn)# group-alias Fra-QA
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または名前の付いたトンネル グループ コンフィギュレーションを消去します。
show webvpn group-alias	指定したトンネル グループまたはすべてのトンネル グループに対するエイリアスを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定するトンネル グループ webvpn コンフィギュレーション モードに入ります。

group-delimiter

グループ名の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したユーザ名からグループ名を解析するときに使用するデリミタを指定するには、グローバル コンフィギュレーション モードで **group-delimiter** コマンドを使用します。このグループ名の解析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。

group-delimiter *delimiter*

no group-delimiter

シンタックスの説明

delimiter	グループ名のデリミタとして使用する文字を指定します。 有効値は、**@**、**#**、および **!** です。

デフォルト

デフォルトでは、デリミタは指定されておらず、グループ名の解析はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このデリミタは、トンネルのネゴシエーション中に、ユーザ名からトンネル グループ名を解析するために使用されます。デフォルトでは、デリミタは指定されておらず、グループ名の解析はディセーブルになっています。

例

次の例は、グループ デリミタを番号記号（#）に変更するための **group-delimiter** コマンドを示しています。

```
hostname(config)# group-delimiter #
```

関連コマンド

コマンド	説明
clear config group-delimiter	設定済みのグループ デリミタを消去します。
show running-config group-delimiter	現在の group-delimiter の値を表示します。
strip-group	strip-group の処理をイネーブルまたはディセーブルにします。

group-lock

リモート ユーザがトンネル グループだけからアクセスできるようにするには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **group-lock** コマンドを発行します。

group-lock アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループ ポリシーから継承できます。group-lock をディセーブルにするには、**group-lock none** コマンドを使用します。

group-lock はユーザを制限するときに、VPN Client に設定されているグループが、ユーザの割り当て先のトンネル グループと同じかどうかを確認します。同じでない場合、セキュリティ アプライアンスは、ユーザが接続できないようにします。group-lock を設定しない場合、セキュリティ アプライアンスは割り当てられているグループを考慮せずにユーザを認証します。

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

シンタックスの説明

none	group-lock をヌル値に設定して、group-lock の制限を拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから group-lock の値を継承しないようにします。
value *tunnel-grp-name*	接続しようとするユーザ用にセキュリティ アプライアンスが必要とする既存のトンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループ ポリシーにグループ ロックを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

ネットワーク オブジェクト グループを追加するには、プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション モードで **group-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

group-object *obj_grp_id*

no group-object *obj_grp_id*

シンタックスの説明

obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。アルファベット、数字、アンダースコア（_）、ハイフン（-）、およびピリオド（.）を任意に組み合せることができます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

group-object コマンドは、**object-group** コマンドと組み合せることで、それ自身がオブジェクト グループであるオブジェクトを定義します。このコマンドは、プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション モードで使用されます。このサブコマンドを使用すると、同じタイプのオブジェクトを論理的にグループ化することや、構造化コンフィギュレーションの階層型オブジェクト グループを構築することができます。

グループ オブジェクトに限り、オブジェクトをオブジェクト グループ内で重複させることができます。たとえば、オブジェクト 1 がグループ A とグループ B の両方にある場合、A と B を両方含むグループ C を定義できます。ただし、グループ オブジェクトに含めることによってグループ階層が循環型になる場合は、含めることができません。たとえば、グループ A をグループ B に含め、同時にグループ B をグループ A に含めることはできません。

階層型オブジェクト グループの最大許容レベルは 10 です。

例

次の例は、ホストを重複させる必要がなくなるように、ネットワーク コンフィギュレーション モードで **group-object** コマンドを使用する方法を示しています。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

group-policy

グループ ポリシーを作成または編集するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを使用します。グループ ポリシーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

シンタックスの説明

external server-group *server_group*	グループ ポリシーを外部として指定し、セキュリティ アプライアンスがアトリビュートをクエリーするための AAA サーバ グループを指定します。
from *group-policy_name*	この内部グループ ポリシーのアトリビュートを、既存のグループ ポリシーの値に初期化します。
internal	グループ ポリシーを内部として指定します。
name	グループ ポリシーの名前を指定します。この名前は最大 64 文字です。スペースを含めることはできません。
password *server_password*	外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定します。このパスワードは最大 128 文字です。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。使用上のガイドラインを参照してください。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

「DefaultGroupPolicy」というデフォルトのグループ ポリシーは、常にセキュリティ アプライアンス上に存在します。しかし、このデフォルトのグループ ポリシーを有効にするには、このポリシーを使用するようにセキュリティ アプライアンスを設定する必要があります。設定方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

group-policy attributes コマンドを使用して、任意のグループ ポリシー アトリビュート値ペアを設定できる config-group-policy モードに入ります。DefaultGroupPolicy には、次のアトリビュート値ペアが含まれています。

アトリビュート	デフォルト値
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

さらに、config-group-policy モードで **webvpn** コマンドを入力するか、**group-policy attributes** コマンドを入力した後、config-group-webvpn モードで **webvpn** コマンドを入力することで、グループ ポリシーに対する webvpn-mode アトリビュートが設定できます。詳細については、**group-policy attributes** コマンドの説明を参照してください。

例

次の例は、「FirstGroup」という内部グループ ポリシーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal
```

次の例は、「ExternalGroup」という外部グループ ポリシー、「BostonAAA」という AAA サーバ グループ、および「12345678」というパスワードを作成する方法を示しています。

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	config-group-policy モードに入ります。このモードでは、指定したグループ ポリシーのアトリビュートと値を設定したり、グループの webvpn アトリビュートを設定する webvpn モードに入ったりできます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

group-policy attributes

config-group-policy モードに入るには、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを使用します。グループ ポリシーからすべてのアトリビュートを削除するには、このコマンドの **no** 形式を使用します。config-group-policy モードで、指定したグループ ポリシーのアトリビュート値ペアの設定、またはグループ ポリシー webvpn コンフィギュレーション モードでのグループの webvpn アトリビュートの設定ができます。

group-policy *name* **attributes**

no group-policy *name* **attributes**

シンタックスの説明

name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

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

- **no** 形式は、アトリビュートを実行コンフィギュレーションから削除し、値を別のグループ ポリシーから継承できるようにします。
- **none** キーワードは、実行コンフィギュレーションのアトリビュートをヌル値に設定して、値を継承できないようにします。
- ブール アトリビュートには、イネーブルまたはディセーブルになっている設定のための明示的なシンタックスがあります。

DefaultGroupPolicy という名前のデフォルト グループ ポリシーは、常にセキュリティ アプライアンスに存在します。しかし、このデフォルトのグループ ポリシーを有効にするには、このポリシーを使用するようにセキュリティ アプライアンスを設定する必要があります。設定方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

group-policy attributes コマンドは、任意のグループ ポリシー アトリビュート値ペアを設定できる config-group-policy モードに入ります。DefaultGroupPolicy には、次のアトリビュート値ペアが含まれています。

アトリビュート	デフォルト値
backup-servers	keep-client-config
banner	none
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

さらに、**group-policy attributes** コマンドを入力した後、config-group-policy モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn-mode アトリビュートが設定できます。詳細については、**webvpn** コマンド（グループ ポリシー アトリビュートおよびユーザ名アトリビュート モード）の説明を参照してください。

例

次の例は、FirstGroup というグループ ポリシーのグループ ポリシー アトリビュート モードに入る方法を示しています。

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

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成、編集、または削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn（グループ ポリシー アトリビュート モード）	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

group-prompt

WebVPN ユーザに対して、セキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのグループ プロンプトをカスタマイズするには、webvpn カスタマイゼーション モードで **group-prompt** コマンドを使用します。

group-prompt {**text** | **style**} *value*

[**no**] **group-prompt** {**text** | **style**} *value*

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

シンタックスの説明

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

デフォルト

グループ プロンプトのデフォルトのテキストは「GROUP:」です。

グループ プロンプトのデフォルトのスタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

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

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

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

例

次の例では、テキストを「Corporate Group:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# group-prompt text Corporate Group:
F1-asa1(config-webvpn-custom)# group-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザ名プロンプトをカスタマイズします。

group-url

グループに対する着信 URL または IP アドレスを指定するには、トンネル グループ WebVPN コンフィギュレーション モードで **group-url** コマンドを使用します。リストから URL を削除するには、このコマンドの **no** 形式を使用します。

group-url *url* [**enable** | **disable**]

no group-url *url*

シンタックスの説明

disable	URL をディセーブルにしますが、リストから削除はしません。
enable	URL をイネーブルにします。
url	このトンネル グループの URL または IP アドレスを指定します。

デフォルト

デフォルトの URL または IP アドレスはありませんが、URL または IP アドレスを指定すると、デフォルトでイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

グループ URL または IP アドレスを指定することで、ログイン時にユーザがグループを選択する必要がなくなります。ユーザがログインすると、セキュリティ アプライアンスは tunnel-group-policy テーブル内のユーザの着信 URL またはアドレスを探します。着信 URL またはアドレスが検出され、さらにトンネル グループで group-url がイネーブルである場合、セキュリティ アプライアンスは関連するトンネル グループを自動的に選択し、ユーザに対してログイン ウィンドウでユーザ名フィールドとパスワード フィールドだけを表示します。このように表示することで、ユーザ インターフェイスが簡素化され、グループのリストがユーザの目に触れないようになるという利点が加わります。ユーザが見るログイン ウィンドウは、トンネル グループに対して設定されたカスタマイゼーションを使用します。

着信 URL またはアドレスがディセーブルで、グループ エイリアスが設定されている場合、グループのドロップダウン リストも表示されるので、ユーザは選択を行う必要があります。

1 つのグループに対して、複数の URL またはアドレスが設定できます（あるいは、何も設定しなくてもかまいません）。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにできます。指定した URL およびアドレスそれぞれに対して、別個の **group-url** コマンドを使用する必要があります。http プロトコルか https プロトコルを含む、URL 全体またはアドレス全体を指定してください。

同じ URL およびアドレスを、複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネル グループに対する URL またはアドレスを受け入れる前に、URL およびアドレスの一意性を確認します。

次の例は、「test」という名前の webvpn トンネル グループを設定し、そのグループに対して 2 つのグループ URL、「http://www.cisco.com」および「https://supplier.com」を確立するコマンドを示しています。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com
hostname(config-tunnel-webvpn)# group-url https://supplier.company.com
hostname(config-tunnel-webvpn)#
```

次の例では、RadiusServer という名前のトンネル グループに対してグループ URL の http://www.cisco.com および http://192.168.10.10 をイネーブルにします。

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または名前の付いたトンネル グループ コンフィギュレーションを消去します。
show webvpn group-url	指定したトンネル グループまたはすべてのトンネル グループに対する URL を表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

h245-tunnel-block

H.323 の H.245 トンネリングをブロックするには、パラメータ コンフィギュレーション モードで **h245-tunnel-block** 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。

h245-tunnel-block action [drop-connection | log]

no h245-tunnel-block action [drop-connection | log]

シンタックスの説明

drop-connection	H.245 トンネルが検出されたときにコール セットアップ接続をドロップします。
log	H.245 トンネルが検出されたときにログを発行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 コールの H.245 トンネリングをブロックする方法を示しています。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# h245-tunnel-block action drop-connection
```

関連コマンド

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

hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムをデフォルト値の SHA-1 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。

hash {**md5** | **sha**}

no hash

シンタックスの説明

md5	IKE ポリシーのハッシュ アルゴリズムを MD5（HMAC バリアント）に指定します。
priority	ポリシーの優先順位を示す固有の番号。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
sha	IKE ポリシーのハッシュ アルゴリズムを SHA-1（HMAC バリアント）に指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy hash** コマンドは既存のものです。
7.2.(1)	**isakmp policy hash** コマンドが、**hash** コマンドに置き換えられました。

使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。

例

次の例は、グローバル コンフィギュレーション モードで、**hash** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーで MD5 ハッシュ アルゴリズムを使用することを指定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# hash md5
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

help

指定したコマンドのヘルプ情報を表示するには、ユーザ EXEC モードで **help** コマンドを使用します。

help {*command* | **?**}

シンタックスの説明

command	CLI ヘルプの表示対象となるコマンドを指定します。
?	現在の特権レベルとモードで利用できるコマンドをすべて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

help コマンドは、すべてのコマンドについてヘルプ情報を表示します。個々のコマンドについてのヘルプは、***help*** コマンドの後にコマンド名を入力することで、表示できます。コマンド名を指定しないで、代わりに ***?*** を入力すると、現在の特権レベルとモードで使用可能なコマンドがすべて表示されます。

pager コマンドがイネーブルになっている場合は、24 行が表示されたときに、表示が一時停止して次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトは UNIX の **more** コマンドと同様のシンタックスを使用します。このシンタックスを次に示します。

- 次のテキスト画面を表示するには、**Space** キーを押す。
- 次の行を表示するには、**Enter** キーを押す。
- コマンドラインに戻るには、**q** キーを押す。

例

次の例は、***rename*** コマンドのヘルプを表示する方法を示しています。

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

次の例は、コマンド名と疑問符を入力してヘルプを表示する方法を示しています。

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

コア コマンド（**show**、**no**、**clear** 以外のコマンド）についてのヘルプは、コマンド プロンプトで **?** を入力します。

```
hostname(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

hic-fail-group-policy

グループ ポリシーを指定して、デフォルトのグループ ポリシーとは異なる WebVPN ユーザ アクセス権限を許可するには、トンネル グループ webvpn コンフィギュレーション モードで **hic-fail-group-policy** コマンドを使用します。このコマンドの **no** 形式は、グループ ポリシーにデフォルトのグループ ポリシーを使用します。

hic-fail-group-policy *name*

no hic-fail-group-policy

シンタックスの説明

name	グループ ポリシーの名前を指定します。

デフォルト

DfltGrpPolicy

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Cisco Secure Desktop がインストールされたセキュリティ アプライアンスだけで有効です。ホストの整合性確認（*System Detection* とも呼ばれる）には、VPN 機能ポリシーを適用するために満たす必要がある基準の最小セットに対するリモート PC のチェックが含まれます。セキュリティ アプライアンスは、リモート CSD ユーザへのアクセス権限を制限するために、hic-fail-group-policy アトリビュートの値を次のように使用します。

- VPN 機能ポリシーを「Use Failure Group-Policy」（失敗グループ ポリシーを使用する）に設定している場合は、常にこの値を使用します。
- VPN 機能ポリシーを「Use Success Group-Policy, if criteria match」（基準が一致する場合に成功グループ ポリシーを使用する）に設定している場合は、基準が一致しなかった時にこの値を使用します。

このアトリビュートは、失敗グループ ポリシーの名前を適用するよう指定します。グループ ポリシーを使用して、アクセス権限を、デフォルトのグループ ポリシーに関連付けられているアクセス権限と区別します。

（注） VPN 機能ポリシーを「Always use Success Group-Policy」（常に成功グループ ポリシーを使用する）に設定している場合、セキュリティ アプライアンスは、このアトリビュートを使用しません。

詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

例

次の例は、「FirstGroup」という名前の WebVPN トンネル グループを作成し、「group2」という名前の失敗グループ ポリシーを指定しています。

```
hostname(config)# tunnel-group FirstGroup webvpn
hostname(config)# tunnel-group FirstGroup webvpn-attributes
hostname(config-tunnel-webvpn)# hic-fail-group-policy group2
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	名前付きのトンネル グループの WebVPN アトリビュートを指定します。

hidden-parameter

セキュリティ アプライアンスが SSO 認証用の認証 Web サーバに送信する HTTP POST 要求に非表示パラメータを指定するには、aaa-server-host コンフィギュレーション モードで **hidden-parameter** コマンドを使用します。

すべての非表示パラメータを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

これは HTTP Forms コマンドを使用した SSO です。

hidden-parameter *string*

no hidden-parameter

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	フォームに組み込まれ、SSO サーバに送信される非表示パラメータです。複数の行に入力できます。各行の最大文字数は、255 文字です。すべての行を一体とした、つまり完全な非表示パラメータの最大文字数は、2048 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、認証 Web サーバに対してシングル サインオン認証要求を送信するために HTTP POST 要求を使用します。その要求には、ユーザに見えない SSO HTML 形式に基づく固有の非表示パラメータが、ユーザ名とパスワード以外に、必要な場合があります。Web サーバから受信したフォームに対して HTTP ヘッダー アナライザを使用することで、POST 要求に含まれると Web サーバが予期している非表示パラメータを検出できます。

コマンド **hidden-parameter** を使用すると、Web サーバが必要とする非表示パラメータを認証 POST 要求に指定できます。ヘッダー アナライザを使用すると、任意の符号化 URL パラメータを含む非表示パラメータ文字列全体をコピー アンド ペーストできます。

入力を簡単にするため、1 つの非表示パラメータを複数の連続した行に入力できます。セキュリティ アプライアンスは、その複数の行を 1 つの非表示パラメータに連結します。非表示パラメータ 1 行の最大文字数は 255 文字ですが、各行にはそれより少ない数の文字を入力できます。

（注）　文字列に疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次の例は、& で区切られた 4 つのフォーム エントリ、およびその値で構成される 1 つの非表示パラメータを示しています。POST 要求から抜き出した 4 つのエントリとその値を次に示します。

- 値が ISO-8859-1 の SMENC
- 値が US-EN の SMLOCALE
- 値が https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG のターゲット
- 値が 0 の smauthreason

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter
SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter
t=https%3A%2F%2Ftools.cisco.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter
o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。
start-url	事前ログイン クッキーの取得先 URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

homepage

この WebVPN ユーザまたはグループ ポリシーに対して、ログイン後すぐに表示する Web ページの URL を指定するには、WebVPN モードで **homepage** コマンドを使用します。WebVPN モードには、グループ ポリシー モードまたはユーザ名モードから入ります。設定済みのホーム ページ（**homepage none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを使用します。

homepage {value *url-string* **| none}**

no homepage

シンタックスの説明

none	WebVPN ホーム ページを使用しないことを指定します。ヌル値を設定して、ホーム ページを拒否します。ホーム ページを継承しないようにします。
value *url-string*	ホーム ページの URL を指定します。文字列は、http:// または https:// で始まる必要があります。

デフォルト

デフォルトのホーム ページはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループ ポリシーのホーム ページとして www.example.com を指定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

host

RADIUS アカウンティングを使用して対話するホストを指定するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **host** コマンドを使用します。このモードには、ポリシー マップ タイプの検査 RADIUS アカウント サブモードで **parameters** コマンドを使用してアクセスできます。

このオプションは、デフォルトではディセーブルになっています。

host *address* [***key*** *secret*]

no host ***address*** [***key secret***]

シンタックスの説明

host	RADIUS アカウンティング メッセージを送信する単一のエンドポイントを指定します。
address	RADIUS アカウンティング メッセージを送信するクライアントまたはサーバの IP アドレス。
key	アカウンティング メッセージの無料コピーを送信するために、エンドポイントの秘密鍵を指定するオプションのキーワード。
secret	メッセージの検証に使用される、アカウンティング メッセージを送信するエンドポイントの共有秘密鍵。この鍵には最大 128 文字の英数字を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、インスタンスを複数設定することができます。

例

次の例では、RADIUS アカウンティングによるホストの指定方法を示しています。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# host 209.165.202.128 key cisco123
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

hostname

セキュリティ アプライアンスのホスト名を設定するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。デフォルトのホスト名に戻すには、このコマンドの **no** 形式を使用します。ホスト名はコマンドライン プロンプトとして表示されます。複数のデバイスに対してセッションを確立している場合は、ホスト名を見ることでコマンドの入力場所を把握できます。

hostname *name*

no hostname [*name*]

シンタックスの説明

name	最大 63 文字のホスト名を指定します。ホスト名の先頭と末尾はアルファベットまたは数字にする必要があります。それ以外の部分に使用できる文字はアルファベット、数字、またはハイフンのみです。

デフォルト

デフォルトのホスト名はプラットフォームによって異なります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	アルファベット以外の文字（ハイフンを除く）が使用不可になりました。

使用上のガイドライン

マルチ コンテキスト モードの場合、システム実行スペースに設定したホスト名は、すべてのコンテキストのコマンドライン プロンプトに表示されます。

コンテキスト内にオプションで設定したホスト名は、コマンドラインに表示されませんが、**banner** コマンドの **$(hostname)** トークンに使用できます。

例

次の例では、ホスト名を firewall1 に設定します。

```
hostname(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
banner	ログイン バナー、「今日のお知らせ」バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。

hsi

H.323 プロトコルの検査のために HSI を HSI グループに追加するには、hsi グループ コンフィギュレーション モードで **hsi** 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。

hsi *ip_address*

no hsi *ip_address*

シンタックスの説明

ip_address	追加するホストの IP アドレス。1 つの HSI グループ当たり最大 5 つの HSI が許可されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査ポリシー マップで HSI を HSI グループに追加する方法を示しています。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi-group	HSI グループを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

hsi-group

H.323 プロトコル検査用に HSI グループを定義し、hsi グループ コンフィギュレーション モードに入るには、パラメータ コンフィギュレーション モードで **hsi-group** 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。

hsi-group *group_id*

no hsi-group *group_id*

シンタックスの説明

group_id	HSI グループ ID 番号（0 ～ 2147483647）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査ポリシー マップで HSI グループを設定する方法を示します。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

html-content-filter

このユーザまたはグループ ポリシーに対して、WebVPN セッションの Java、ActiveX、イメージ、スクリプト、クッキーをフィルタリングするには、WebVPN モードで **html-content-filter** コマンドを使用します。WebVPN モードには、グループ ポリシー モードまたはユーザ名モードから入ります。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を使用します。すべてのコンテンツ フィルタ（**html-content-filter none** コマンドを発行して作成されたヌル値を含む）を削除するには、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。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。html コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを使用します。

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

シンタックスの説明

cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを実現します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java と ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> タグを削除します）。
none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除します）。

デフォルト

フィルタリングは行われません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コマンドを 2 回使用すると、先行する設定値が上書きされます。

例

次の例は、FirstGroup というグループ ポリシーに対して、JAVA、ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
```

関連コマンド

コマンド	説明
webvpn（グループ ポリシー、ユーザ名）	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

http

セキュリティ アプライアンスの内部にある HTTP サーバにアクセスできるホストを指定するには、グローバル コンフィギュレーション モードで **http** コマンドを使用します。1 つまたは複数のホ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。このアトリビュートをコンフィギュレーションから削除するには、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。

http *ip_address subnet_mask interface_name*

no http

シンタックスの説明

interface_name	ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスの名前を指定します。
ip_address	HTTP サーバにアクセスできるホストの IP アドレスを指定します。
subnet_mask	HTTP サーバにアクセスできるホストのサブネット マスクを指定します。

デフォルト

HTTP サーバにアクセスできるホストは指定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、IP アドレス 10.10.99.1 およびサブネット マスク 255.255.255.255 のホストが外部インターフェイス経由で HTTP サーバにアクセスできるようにする方法を示しています。

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

次の例は、すべてのホストが外部インターフェイス経由で HTTP サーバにアクセスできるようにする方法を示しています。

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http authentication-certificate

HTTPS 接続を確立しようとするユーザに、証明書による認証を要求するには、グローバル コンフィギュレーション モードで **http authentication-certificate** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。コンフィギュレーションからすべての **http authentication-certificate** コマンドを削除するには、引数を指定しないで **no** 形式を使用します。

セキュリティ アプライアンスは、PKI トラストポイントに対して証明書を検証します。証明書が検証に合格しなかった場合、セキュリティ アプライアンスは SSL 接続を閉じます。

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

シンタックスの説明

interface	証明書認証を要求するセキュリティ アプライアンス上のインターフェイスを指定します。

デフォルト

HTTP 証明書認証はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

URL は検証後に判明します。そのため、検証は WebVPN と ASDM アクセスの両方に影響します。

ASDM は、この値のほかに、独自の認証方式を使用します。つまり、証明書認証とユーザ名 / パスワード認証の両方が設定されている場合は、両方の認証を要求し、証明書認証がディセーブルの場合は、ユーザ名 / パスワード認証のみを要求します。

例

次の例は、outside と external というインターフェイスに接続しようとするクライアントに証明書認証を要求する方法を示しています。

```
hostname(config)# http authentication-certificate inside
hostname(config)# http authentication-certificate external
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http-comp

特定のグループまたはユーザに対して WebVPN 接続を通して http データの圧縮をイネーブルにするには、グループ ポリシーまたはユーザ名の webvpn モードで **http-comp** コマンドを使用します。

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

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

シンタックスの説明

gzip	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	グループまたはユーザに対して圧縮をディセーブルにすることを指定します。

デフォルト

デフォルトでは、圧縮は *gzip* に設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

WebVPN 接続では、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシーまたはユーザ名の webvpn モードで設定された **http-comp** コマンドを上書きします。

例

次の例では、グループ ポリシー sales に対して圧縮がディセーブルにされます。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、IPSec VPN 接続に対して圧縮をイネーブルにします。

http-proxy

HTTP プロキシ サーバを設定するには、WebVPN モードで **http-proxy** コマンドを使用します。HTTP プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

このプロキシ サーバは、セキュリティ アプライアンスが HTTP 要求に使用する外部プロキシ サーバです。

http-proxy *address* [*port*]

no http-proxy

シンタックスの説明

address	外部 HTTP プロキシ サーバの IP アドレスを指定します。
port	HTTP プロキシ サーバが使用するポートを指定します。デフォルト ポートは 80 です。値を指定しない場合、セキュリティ アプライアンスはこのポートを使用します。

デフォルト

HTTP プロキシ サーバは、デフォルトでは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、ポート 80 を使用する IP アドレス 10.10.10.7 の HTTP プロキシ サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 10.10.10.7
hostname(config-webvpn)
```

http redirect

セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定するには、グローバル コンフィギュレーション モードで **http redirect** コマンドを使用します。指定した http redirect コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。すべての http redirect コマンドをコンフィギュレーションから削除するには、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。

http redirect *interface* [*port*]

no http redirect [*interface*]

シンタックスの説明

interface	セキュリティ アプライアンスが HTTPS にリダイレクトする HTTP 要求を受信するインターフェイスを指定します。
port	セキュリティ アプライアンスが HTTP 要求をリッスンするポートを指定します。HTTP 要求は後で HTTPS にリダイレクトされます。デフォルトでは、ポート 80 上でリッスンします。

デフォルト

HTTP リダイレクトはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このインターフェイスが、HTTP を許可するアクセス リストを要求します。アクセス リストがない場合、セキュリティ アプライアンスは、ポート 80 も、HTTP 用に設定した他のどのポートもリッスンしません。

例

次の例は、デフォルト ポート 80 のままで、内部インターフェイスの HTTP リダイレクトを設定する方法を示しています。

```
hostname(config)# http redirect inside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http server enable

セキュリティ アプライアンス HTTP サーバ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 **http server enable** コマンドを使用します。HTTP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

http server enable [*port*]

シンタックスの説明

port	HTTP 接続に使用するポート。範囲は 1 ～ 65535 です。デフォルト ポートは 443 です。

デフォルト

HTTP サーバはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、HTTP サーバをイネーブルにする方法を示しています。

```
hostname(config)# http server enable
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

https-proxy

HTTPS プロキシ サーバを設定するには、WebVPN モードで **https-proxy** コマンドを使用します。HTTPS プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの no 形式を使用します。

このプロキシ サーバは、セキュリティ アプライアンスが HTTPS 要求に使用する外部プロキシ サーバです。

https-proxy *address* [*port*]

no https-proxy

シンタックスの説明

address	外部 HTTPS プロキシ サーバの IP アドレスを指定します。
port	HTTPS プロキシ サーバが使用するポートを指定します。デフォルト ポートは 443 です。値を指定しない場合、セキュリティ アプライアンスはこのポートを使用します。

デフォルト

HTTPS プロキシ サーバは、デフォルトでは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

例

次の例は、ポート 443 を使用する IP アドレス 10.10.10.1 の HTTPS プロキシ サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 10.10.10.1 443
```

hw-module module password-reset

ハードウェア モジュールのパスワードをデフォルト値「cisco」にリセットするには、特権 EXEC モードで **hw-module module password reset** コマンドを使用します。

hw-module module slot# ***password-reset***

シンタックスの説明

slot#	スロット番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効となるのは、ハードウェア モジュールが Up 状態にあり、パスワード リセットをサポートしている場合のみです。AIP SSM に対してこのコマンドを実行すると、AIP SSM はリブートします。このモジュールはリブートが完了するまでオフラインになります。これには数分間かかる場合があります。**show module** コマンドを実行すると、モジュールの状態を監視できます。

このコマンドは、確認のためのプロンプトを常に表示します。コマンドが正常に完了した場合、その他の出力は表示されません。コマンドが失敗した場合、障害が発生した理由を説明するエラー メッセージが表示されます。表示されるエラー メッセージを次に示します。

```
Unable to reset the password on the module in slot 1
Unable to reset the password on the module in slot 1 - unknown module state
Unable to reset the password on the module in slot 1 - no module installed
Failed to reset the password on the module in slot 1 - module not in Up state
Unable to reset the password on the module in slot 1 - unknown module type
The module is slot [n] does not support password reset
Unable to reset the password on the module in slot 1 - no application found
The SSM application version does not support password reset
Failed to reset the password on the module in slot 1
```

例

次の例では、slot 1 のハードウェア モジュールのパスワードをリセットします。

```
hostname (config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module reset	SSM ハードウェアをシャットダウンし、リセットします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module recover

TFTP サーバからインテリジェント SSM（たとえば、AIP SSM）にリカバリ ソフトウェア イメージをロードする場合や、TFTP サーバにアクセスするためのネットワーク設定値を設定する場合は、特権 EXEC モードで **hw-module module recover** コマンドを使用します。SSM でローカル イメージをロードできないような場合は、このコマンドを使用して SSM を回復することが必要となる場合があります。このコマンドは、インターフェイスの SSM（4GE SSM など）に対しては使用できません。

hw-module module 1 recover {***boot*** | ***stop*** | ***configure*** [***url*** *tfp_url* | ***ip*** *port_ip_address* | ***gateway*** *gateway_ip_address* | ***vlan*** *vlan_id*]}

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。
boot	この SSM のリカバリを開始し、***configure*** 設定に応じてリカバリ イメージをダウンロードします。その後、SSM が新しいイメージからリブートされます。
configure	リカバリ イメージをダウンロードするためのネットワーク パラメータを設定します。***configure*** キーワードの後ろにネットワーク パラメータを入力しない場合は、情報を入力するよう求められます。
gateway *gateway_ip_address*	（オプション）SSM 管理インターフェイスを通じて TFTP サーバにアクセスするためのゲートウェイ IP アドレス。
ip *port_ip_address*	（オプション）SSM 管理インターフェイスの IP アドレス。
stop	リカバリ アクションを停止し、リカバリ イメージのダウンロードを停止します。SSM　は元のイメージからブートします。このコマンドは、**hw-module module boot** コマンドを使用してリカバリを開始してから 30 ～ 45 秒以内に入力する必要があります。この期間を過ぎてから **stop** コマンドを発行すると、SSM が応答しなくなるなど、予期しない結果が生じる場合があります。
url *tfp_url*	（オプション）TFTP サーバ上のイメージの URL。この形式は次のとおりです。 ***tftp://****server/*[*path/*]*filename*
vlan *vlan_id*	（オプション）管理インターフェイスの VLAN ID を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用できるのは、SSM が Up、Down、Unresponsive、または Recovery 状態にある場合のみです。状態については、**show module** コマンドを参照してください。

例

次の例では、TFTP サーバからイメージをダウンロードするように SSM を設定します。

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

次の例では、SSM を回復します。

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module reload

インテリジェント SSM ソフトウェア（たとえば、AIP SSM）をリロードするには、特権 EXEC モードで **hw-module module reload** コマンドを使用します。このコマンドは、インターフェイスの SSM（4GE SSM など）に対しては使用できません。

hw-module module 1 ***reload***

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効となるのは、SSM の状態が Up の場合のみです。状態については、**show module** コマンドを参照してください。

このコマンドは、同じくハードウェア リセットを実行する **hw-module module reset** コマンドとは異なります。

例

次の例では、スロット 1 の SSM をリロードします。

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module reset

SSM ハードウェアをシャットダウンし、リセットするには、特権 EXEC モードで **hw-module module reset** コマンドを使用します。

hw-module module 1 ***reset***

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効となるのは、SSM の状態が Up、Down、Unresponsive、または Recover の場合のみです。状態については、**show module** コマンドを参照してください。

SSM が Up 状態にある場合、**hw-module module reset** コマンドを使用すると、リセットする前にソフトウェアをシャットダウンするよう求められます。

インテリジェント SSM（たとえば、AIP SSM）を回復するには、**hw-module module recover** コマンドを使用します。SSM が Recover 状態にあるときに **hw-module module reset** を入力しても、SSM はリカバリ プロセスを中断しません。**hw-module module reset** コマンドは、SSM のハードウェア リセットを実行します。ハードウェア リセット後に、SSM のリカバリが続行されます。SSM がハングした場合は、リカバリ中でも SSM をリセットできます。ハードウェア リセットにより、問題が解決する場合があります。

このコマンドは、ソフトウェアのリロードのみを行いハードウェア リセットを行わない **hw-module module reload** コマンドとは異なります。

例

次の例では、Up 状態にあるスロット 1 の SSM をリセットします。

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module shutdown

SSM ソフトウェアをシャットダウンするには、特権 EXEC モードで **hw-module module shutdown** コマンドを使用します。

hw-module module 1 shutdown

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSM ソフトウェアをシャットダウンすると、コンフィギュレーション データを失わずに SSM の電源を安全にオフにできる状態になります。

このコマンドが有効となるのは、SSM の状態が Up または Unresponsive の場合のみです。状態については、**show module** コマンドを参照してください。

例

次の例では、スロット 1 の SSM をシャットダウンします。

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
show module	SSM 情報を表示します。