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。設定を削除するには、このコマンドの **no** 形式を使用します。

gateway *ip_address* [*group_id*]

構文の説明

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、デフォルトでディセーブルになっています。

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	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

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、**gateway** コマンドを使用します。*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* オプションには 0 ～ 4294967295 の数字を指定します。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

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
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 の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の情報を表示します。

global

NAT 用にマッピング先の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**}

構文の説明

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。インターフェイス アドレスを使用する必要がある場合はこのキーワードを使用しますが、アドレスは、DHCP を使用してダイナミックに割り当てられます。
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から出るときに実アドレスの変換先となる、マッピング先のアドレス（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、変換対象の実アドレスにマッピング プールを関連付けるために、**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。 NAT ID 0 に対して **global** コマンドを指定しないでください。0 は、アイデンティティ NAT および NAT 免除用に予約されており、これらの NAT では **global** コマンドは使用しません。
netmask *mask*	（任意）*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* と組み合わせた場合には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	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
8.0(2)	NAT は、トランスペアレント ファイアウォール モードでサポートされるようになりました。

使用上のガイドライン

ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 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、1 つの **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まで待たずに新しい NAT 情報を使用するために、**clear xlate** コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、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-alias

ユーザがトンネル グループの参照に使用する 1 つ以上の変換名を作成するには、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*

構文の説明

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。選択した任意のストリングを指定できます。ただし、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	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 エイリアスが、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。各グループに複数のエイリアスを指定することも、エイリアスを指定しないことも可能です。このコマンドは、同じグループが「Devtest」や「QA」などの複数の一般名で知られている場合に役立ちます。

例

次に、「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の例を示します。

```
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指定したトンネル グループ設定をクリアします。
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 グループのエイリアスを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定するためのトンネル グループ webvpn コンフィギュレーション モードを開始します。

group-delimiter

グループ名の解析をイネーブルにして、トンネルのネゴシエート時に受信したユーザ名からグループ名を解析する場合に使用するデリミタを指定するには、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

構文の説明

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。 有効な値は、**@**、**#**、および **!** です。

デフォルト

デフォルトで、デリミタは指定されていないため、グループ名解析はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

デリミタは、トンネルがネゴシエートされるときに、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、デリミタは指定されていないため、グループ名解析はディセーブルです。

例

次に、グループ デリミタをハッシュ マスク（#）に変更する **group-delimiter** コマンドの例を示します。

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

関連コマンド

コマンド	説明
clear configure group-delimiter	設定したグループ デリミタをクリアします。
show running-config group-delimiter	現在のグループ デリミタ値を表示します。
strip-group	グループ除去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 グループを介してしかアクセスできないように制限するには、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。

実行コンフィギュレーションから **group-lock** 属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

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

no group-lock

構文の説明

none	group-lock をヌル値に設定します。これにより、グループ ロックの制限が許可されなくなります。デフォルトまたは指定したグループ ポリシーの group-lock 値を継承しないようにします。
value *tunnel-grp-name*	ユーザが接続する際にセキュリティ アプライアンスによって要求される既存のトンネル 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	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—
ユーザ名コンフィギュレーション	•	—	•	—	—

使用上のガイドライン

グループ ロック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。

グループ ロックは、VPN クライアントに設定されているグループが、ユーザが割り当てられているトンネル グループと同一であるかどうかをチェックすることによって、ユーザを制限します。同一ではなかった場合、セキュリティ アプライアンスはユーザによる接続を禁止します。グループ ロックを設定しなかった場合、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に関係なくユーザを認証します。

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

次に、FirstGroup という名前のグループ ポリシーにグループ ロックを設定する例を示します。

```
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 タイプ 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*

構文の説明

obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。

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	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、ICMP タイプ 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
既存	このコマンドは既存です。

使用上のガイドライン

group-object コマンドは、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するために、**object-group** コマンドとともに使用します。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 タイプ コンフィギュレーション モードで使用します。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グループ化して、構造化されたコンフィギュレーションの階層オブジェクト グループを構築できます。

オブジェクト グループ内でのオブジェクトの重複は、それらのオブジェクトがグループ オブジェクトの場合は許可されます。たとえば、オブジェクト 1 がグループ A とグループ B の両方に存在する場合、A と B の両方を含むグループ C を定義できます。ただし、グループの階層が循環型になるようなグループ オブジェクトを含めることはできません。たとえば、グループ A にグループ B を含め、さらにグループ B にグループ A を含めることはできません。

階層オブジェクト グループは 10 レベルまで許可されています。

（注） セキュリティ アプライアンスでは IPv6 のネスト化したオブジェクト グループはサポートしていません。このため、そのようなグループ内に属する IPv6 エンティティを持つオブジェクトが別の IPv6 オブジェクト グループに含まれる場合、このオブジェクトに対しては **group-object** コマンドを使用できません。

例

次に、ネットワーク コンフィギュレーション モードで **group-object** コマンドを使用して、ホストを重複させる必要性を排除する例を示します。

```
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。コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 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*

構文の説明

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 アプライアンスが属性を照会する AAA サーバ グループを識別します。
from *group-policy_name*	この内部グループ ポリシーの属性を、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識別します。
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、スペースを含めることができます。スペースを含むグループ名は、二重引用符で囲む必要があります（"Sales Group" など）。
password *server_password*	外部 AAA サーバ グループから属性を取得する際に使用するパスワードを指定します。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	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

セキュリティ アプライアンスには、「DefaultGroupPolicy」という名前のデフォルト グループ ポリシーが常に存在しています。ただし、このデフォルト グループ ポリシーは、これを使用するようにセキュリティ アプライアンスを設定しない限り、有効ではありません。設定手順については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

group-policy attributes コマンドを使用して設定グループ ポリシー モードを開始します。このモードでは、グループ ポリシーのあらゆる属性値ペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	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 分
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

また、設定グループ ポリシーモードで **webvpn** コマンドを入力するか、**group-policy attributes** コマンドを入力してから、設定グループ webvpn モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn モード属性を設定できます。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

次に、「FirstGroup」という名前の内部グループ ポリシーを作成する例を示します。

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

次に、AAA サーバ グループ「BostonAAA」およびパスワード「12345678」を指定して、「ExternalGroup」という名前の外部グループ ポリシーを作成する例を示します。

```
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	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または webvpn モードでのグループの webvpn 属性の設定ができます。
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	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

group-policy attributes

設定グループ ポリシー モードを開始するには、グローバル コンフィギュレーション モードで **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属性を削除するには、このコマンドの **no** バージョンを使用します。設定グループ ポリシー モードでは、指定したグループ ポリシーの属性値ペアを設定したり、グループ ポリシー webvpn コンフィギュレーション モードを開始してグループの webvpn 属性を設定したりできます。

group-policy *name* **attributes**

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

構文の説明

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	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

属性モードのコマンド構文には、一般的に、次のような特徴があります。

- **no** 形式は実行コンフィギュレーションから属性を削除し、別のグループ ポリシーからの値の継承をイネーブルにします。
- **none** キーワードは実行コンフィギュレーションの属性をヌル値に設定し、これによって継承を禁止します。
- ブール型属性には、イネーブルおよびディセーブルの設定用に明示的な構文があります。

セキュリティ アプライアンスには、DefaultGroupPolicy という名前のデフォルト グループ ポリシーが常に存在しています。ただし、このデフォルト グループ ポリシーは、これを使用するようにセキュリティ アプライアンスを設定しない限り、有効ではありません。設定手順については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。

group-policy attributes コマンドを使用して設定グループ ポリシー モードを開始します。このモードでは、グループ ポリシーのあらゆる属性値ペアを設定できます。DefaultGroupPolicy には、次の属性と値のペアがあります。

属性	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 分
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

また、**group-policy attributes** コマンドを入力してから、設定グループ ポリシー 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 モード属性を設定できます。詳細については、**webvpn** コマンド（グループ ポリシー属性モードおよびユーザ名属性モード）の説明を参照してください。

例

次に、FirstGroup という名前のグループ ポリシーのグループ ポリシー属性モードを開始する例を示します。

```
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 ポリシー属性モード）	設定グループ webvpn モードを開始します。このモードで、指定したグループに対する WebVPN 属性を設定できます。

group-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示される 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 コンフィギュレーション モードで **group-prompt** コマンドを使用します。コンフィギュレーションからコマンドを削除して、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。

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

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

構文の説明

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 テキストは「GROUP:」です。

グループ プロンプトのデフォルト 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	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

style オプションは有効な Cascading Style Sheet（CSS）パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。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 で入手できます。

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）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番め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 を使用することを推奨します。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ための便利な機能があります。

例

次に、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 に変更する例を示します。

```
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-search-timeout

show ad-groups コマンドを使用して照会した Active Directory サーバからの応答を待機する最大時間を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **group-search-timeout** コマンドを使用します。コンフィギュレーションから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。

group-search-timeout *seconds*

no group-search-timeout *seconds*

構文の説明

seconds	Active Directory サーバからの応答を待機する時間（1 ～ 300 秒）。

デフォルト

デフォルトは 10 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

show ad-groups コマンドは LDAP を使用している Active Directory サーバにのみ適用され、Active Directory サーバでリストされているグループが表示されます。**group-search-timeout** コマンドを使用して、サーバからの応答を待機する時間を調整します。

例

次に、タイムアウトを 20 秒に設定する例を示します。

```
hostname(config-aaa-server-host)#group-search-timeout 20
```

関連コマンド

コマンド	説明
ldap-group-base-dn	サーバが、ダイナミック グループ ポリシーで使用されるグループの検索を開始する Active Directory 階層のレベルを指定します。
show ad-groups	Active Directory サーバ上でリストされるグループを表示します。

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*

構文の説明

disable	URL をディセーブルにしますが、リストからは削除しません。
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、これ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	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

グループの URL または IP アドレスを指定すると、ユーザがログイン時に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 アプライアンスはトンネル グループ ポリシー テーブル内でユーザの着信 URL/アドレスを検索します。URL/アドレスが見つかり、さらにトンネル グループで group-url がイネーブルになっている場合、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て、ユーザ名およびパスワード フィールドだけをログイン ウィンドウでユーザに表示します。これによりユーザ インターフェイスが簡素化され、グループ リストがユーザに表示されなくなるという利点が追加されます。ユーザに表示されるログイン ウィンドウでは、そのトンネル グループ用に設定されているカスタマイゼーションが使用されます。

URL/アドレスがディセーブルで、group-alias が設定されている場合は、グループのドロップダウン リストも表示され、ユーザによる選択が必要になります。

1 つのグループに対して複数の URL/アドレスを設定する（または、1 つも設定しない）ことができます。URL/アドレスごとに個別にイネーブルまたはディセーブルに設定できます。指定した URL/アドレスごとに個別の **group-url** コマンドを使用する必要があります。http または https プロトコルを含めて、URL/アドレス全体を指定する必要があります。

複数のグループに同じ URL/アドレスを関連付けることはできません。セキュリティ アプライアンスでは、URL/アドレスの一意性を検証してから、トンネル グループに対する URL/アドレスを受け入れます。

次に、「test」という名前の webvpn トンネル グループを設定して、「http://www.cisco.com」および「https://supplier.com」という 2 つのグループ URL をそのグループ用に確立する例を示します。

```
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)#
```

次に、RadiusServer という名前のトンネル グループに対して、グループ URL、http://www.cisco.com および http://192.168.10.10 をイネーブルにする例を示します。

```
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指定したトンネル グループ設定をクリアします。
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 グループの URL を表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ属性を設定する設定 webvpn モードを開始します。

h245-tunnel-block

H.323 で 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]

構文の説明

drop-connection	H.245 トンネルが検出された場合、コール設定接続をドロップします。
log	H.245 トンネルが検出された場合、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	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

次に、H.323 コールで H.245 トンネリングをブロックする例を示します。

```
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 マップのクラス 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インスペクション 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	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hello-interval

インターフェイス上で送信される EIGRP hello パケット間の間隔を指定するには、インターフェイス コンフィギュレーション モードで **hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hello-interval eigrp *as-number seconds*

no hello-interval eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。
seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。

デフォルト

デフォルトの *seconds* は 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、ルーティング トラフィックの増加につながります。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hold-time	hello パケットでアドバタイズされる EIGRP ホールド タイムを設定します。

help

指定する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* | **?**}

構文の説明

command	CLI ヘルプを表示するコマンドを指定します。
?	現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。

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	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です。

使用上のガイドライン

help コマンドを使用すると、すべてのコマンドのヘルプ情報が表示されます。**help** コマンドの後にコマンド名を入力することによって、個々のコマンドのヘルプを参照できます。コマンド名を指定せず、その代わりに **?** と 入力した場合、現在の特権レベルおよびモードで使用可能なすべてのコマンドを表示します。

pager コマンドがイネーブルの場合、24 行表示されると、リスト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 プロンプトでは、次のように、UNIX の **more** コマンドに類似した構文が使用されます。

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

例

次に、**rename** コマンドのヘルプを表示する例を示します。

```
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#
```

次に、コマンド名と疑問符を入力して、ヘルプを表示する例を示します。

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

コマンド プロンプトで **?** を入力すると、主要コマンド（**show**、**no**、または **clear** コマンド以外）に関する ヘルプを表示できます。

```
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（非推奨）

グループ ポリシーを指定して、デフォルト グループ ポリシーとは異なる WebVPN ユーザ アクセス権限を取得するには、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** 形式を使用すると、グループ ポリシーがデフォルト グループ ポリシーに設定されます。

hic-fail-group-policy *name*

no hic-fail-group-policy

構文の説明

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	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。
8.0(2)	このコマンドは廃止されました。

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ているセキュリティ アプライアンスにのみ有効です。*システム検知*とも呼ばれるホストの整合性チェックには、VPN 機能ポリシーを適用するために満たす必要がある最小セットの基準がリモート PC に備わっているかどうかのチェックが含まれています。セキュリティ アプライアンスは、次のように hic-fail-group-policy 属性の値を使用して、リモート CSD ユーザへのアクセス権限を制限します。

- VPN 機能ポリシーを「Use Failure Group-Policy」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」に設定している場合は、基準が一致しなかったときに、この値を使用します。

この属性は、適用される失敗グループ ポリシーの名前を指定します。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 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」に設定している場合、セキュリティ アプライアンスではこの属性を使用しません。

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

次に、「FirstGroup」という名前の WebVPN トンネル グループを作成して、「group2」という名前の失敗グループ ポリシーを指定する例を示します。

```
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	指定したトンネル グループの WebVPN 属性を指定します。

hidden-parameter

セキュリティ アプライアンスが SSO 認証のために認証 Web サーバに送信する HTTP POST 要求の非表示パラメータを指定するには、AAA サーバ ホスト 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。実行コンフィギュレーションからすべての非表示パラメータを削除するには、このコマンドの **no** 形式を使用します。

hidden-parameter *string*

no hidden-parameter

（注） HTTP プロトコルを使用して SSO を正しく設定するには、認証と HTTP プロトコル交換についての詳しい実務知識が必要です。

構文の説明

string	フォームに組み込まれて SSO サーバに送信される非表示パラメータ。複数行に入力できます。各行の最大文字数は 255 です。すべての行をあわせた（非表示パラメータ全体の）最大文字数は 2048 文字です。

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	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

これは HTTP フォームのコマンドを使用した SSO です。

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、認証 Web サーバにシングル サインオン認証要求を送信します。その要求では、ユーザには表示されない SSO HTML フォームの特定の非表示パラメータ（ユーザ名およびパスワード以外）が必要になることがあります。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、Web サーバが POST 要求で想定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 サーバが認証 POST 要求で必要としている非表示パラメータを指定できます。ヘッダー アナライザを使用する場合は、エンコーディング済みの URL パラメータを含む非表示パラメータ ストリング全体をコピーして貼り付けることができます。

入力を簡単にするために、複数の連続行で非表示パラメータを入力できます。セキュリティ アプライアンスでは、その複数行を連結して単一の非表示パラメータにします。非表示パラメータ 1 行ごとの最大文字数は 255 文字ですが、各行にはそれより少ない文字しか入力できません。

（注） ストリング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

次に、& で区切られた 4 つのフォーム エントリとその値で構成される非表示パラメータの例を示します。POST 要求から抜き出された 4 つのエントリおよびその値は、次のとおりです。

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

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およびパスワードを受信するための 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 要求パラメータの名前を指定します。
start-url	プリログイン クッキーを取得する 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。

hidden-shares

CIFS ファイルの非表示共有の可視性を制御するには、設定グループ webvpn コンフィギュレーション モードで **hidden-shares** コマンドを使用します。非表示共有オプション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。

hidden-shares {none | visible}

[no] hidden-shares {none | visible}

構文の説明

none	設定済みの非表示共有の表示およびアクセスをユーザが実行できないことを指定します。
visible	非表示共有を表示して、ユーザがアクセスできるようにします。

デフォルト

このコマンドのデフォルト動作は none 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。

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
8.0(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

非表示共有は、共有名の末尾のドル記号（$）で識別されます。たとえば、ドライブ C は C$ として共有されます。非表示共有では、共有フォルダは表示されず、ユーザはこれらの非表示リソースを参照またはアクセスすることを禁止されます。

hidden-shares コマンドの **no** 形式を使用すると、コンフィギュレーションからオプションが削除され、グループ ポリシー属性として非表示共有がディセーブルになります。

例

次に、GroupPolicy2 に関連する WebVPN CIFS 非表示共有を可視にする例を示します。

```
hostname(config)# webvpn
hostname(config-group-policy)#  group-policy GroupPolicy2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# hidden-shares visible
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
debug webvpn cifs	CIFS に関するデバッグ メッセージを表示します。
group-policy attributes	設定グループ ポリシー モードを開始します。このモードでは、指定したグループ ポリシーへの属性と値の設定、または WebVPN モードでのグループの WebVPN 属性の設定ができます。
url-list	（グローバル コンフィギュレーション モード）WebVPN ユーザがアクセスする URL のセットを設定します。
url-list	（WebVPN モード）WebVPN サーバおよび URL のリストを特定のユーザまたはグループ ポリシーに適用します。

hold-time

セキュリティ アプライアンスが EIGRP hello パケットでアドバタイズするホールド タイムを指定するには、インターフェイス コンフィギュレーション モードで **hold-time** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

hold-time eigrp *as-number seconds*

no hold-time eigrp *as-number seconds*

構文の説明

as-number	EIGRP ルーティング プロセスの自律システム番号です。
seconds	ホールド タイムを秒数で指定します。有効な値は、1 ～ 65535 秒です。

デフォルト

デフォルトの *seconds* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(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

この値は、セキュリティ アプライアンスによって EIGRP hello パケットでアドバタイズされます。そのインターフェイスの EIGRP ネイバーは、この値を使用してセキュリティ アプライアンスの可用性を判断します。アドバタイズされたホールド タイム中にセキュリティ アプライアンスから hello パケットを受信しなかった場合、EIGRP ネイバーはセキュリティ アプライアンスが使用不可であると見なします。

非常に混雑した大規模ネットワークでは、一部のルータおよびアクセス サーバが、デフォルト ホールド タイム内にネイバーから hello パケットを受信できない可能性があります。この場合、ホールド タイムを増やすこともできます。

ホールド タイムは、少なくとも hello 間隔の 3 倍にすることを推奨します。指定したホールド タイム内にセキュリティ アプライアンスで hello パケットを受信しなかった場合、このネイバーを通過するルートは使用不可であると見なされます。

ホールド タイムを増やすと、ネットワーク全体のルート収束が遅くなります。

例

次の例では、EIGRP hello 間隔を 10 秒に、ホールド タイムを 30 秒に設定します。

```
hostname(config-if)# hello-interval eigrp 100 10
hostname(config-if)# hold-time eigrp 100 30
```

関連コマンド

コマンド	説明
hello-interval	インターフェイス上で送信される EIGRP hello パケット間の間隔を指定します。

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時に表示される 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。このモードはグループ ポリシー モードまたはユーザ名モードから開始します。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るようになります。ホームページの継承を禁止するには、**homepage none** コマンドを使用します。

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

no homepage

構文の説明

none	WebVPN ホームページが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。http:// または https:// のいずれかで始まるストリングにする必要があります。

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	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

グループ ポリシーに関連付けられているユーザのホームページ URL を指定するには、このコマンドで url-string の値を入力します。デフォルト グローバル ポリシーからホームページを継承するには、このコマンドの **no** 形式を使用します。クライアントレス ユーザには、認証の成功後すぐにこのページが表示されます。AnyConnect は、VPN 接続が正常に確立されると、この URL に対してデフォルトの Web ブラウザを起動します。Linux プラットフォームでは、AnyConnect が現在このコマンドをサポートしていないため、コマンドは無視されます。

例

次に、FirstGroup という名前のグループ ポリシーのホームページとして www.example.com を指定する例を示します。

```
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 モードを開始して、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。このモードにアクセスするには、ポリシー マップ タイプ インスペクションの RADIUS アカウンティング サブモードで **parameters** コマンドを使用します。指定したホストをディセーブルにするには、このコマンドの **no** 形式を使用します。このオプションは、デフォルトで無効です。

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

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

構文の説明

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 メッセージの無償コピーを送信するエンドポイントの秘密キー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キー。最大 128 の英数字を使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド 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	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できます。

例

次に、RADIUS アカウンティングを使用するホストを指定する例を示します。

```
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インスペクションを設定します。
parameters	インスペクション 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、複数のデバイスへのセッションを確立している場合に、コマンドを入力している場所を把握するのに役立ちます。

hostname *name*

no hostname [*name*]

構文の説明

name	ホスト名を最大 63 文字で指定します。ホスト名はアルファベットまたは数字で開始および終了する必要があり、間の文字にはアルファベット、数字、またはハイフンのみを使用する必要があります。

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	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)	英数字以外の文字（ハイフンを除く）は使用できなくなりました。

使用上のガイドライン

マルチコンテキスト モードでは、システム実行スペースで設定したホスト名がすべてのコンテキストのコマンド ラインのプロンプトに表示されます。

コンテキスト内に任意で設定したホスト名は、コマンドラインには表示されませんが、**banner** コマンドの **$(hostname)** トークンでは使用できます。

例

次に、ホスト名を firewall1 に設定する例を示します。

```
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、Message-of-The-Day 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 インスペクションの HSI グループに HSI を追加するには、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*

構文の説明

ip_address	追加するホストの IP アドレス。HSI グループごとに最大で 5 つの HSI 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	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

次に、H.323 インスペクション ポリシー マップで HSI を HSI グループに追加する例を示します。

```
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	現在のポリシー マップ コンフィギュレーションをすべて表示します。

hsi-group

H.323 プロトコル インスペクション用の HSI グループを定義して、HSI コンフィギュレーション モードを開始するには、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*

構文の説明

group_id	HSI グループの 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	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

次に、H.323 インスペクション ポリシー マップで HSI グループを設定する例を示します。

```
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	現在のポリシー マップ コンフィギュレーションをすべて表示します。

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、およびクッキーをフィルタリングするには、webvpn コンフィギュレーション モードで **html-content-filter** コマンドを使用します。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。

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

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

構文の説明

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提供します。
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 および 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	フィルタリングを行わ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	透過	シングル	コンテキスト	システム
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
7.0(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

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、このコマンドの **no** 形式を引数なしで使用します。**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るようになります。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。

次回このコマンドを使用すると、前回までの設定が上書きされます。

例

次に、FirstGroup という名前のグループ ポリシーに対して JAVA と 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例を示します。

```
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 モードを開始して、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 のグローバル設定を設定できます。

http

セキュリティ アプライアンス内部の 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 つ以上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。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を引数なしで使用します。

http *ip_address subnet_mask interface_name*

no http

構文の説明

interface_name	ホストが HTTP サーバにアクセスするために通過するセキュリティ アプライアンスの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	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です。

例

次に、IP アドレス 10.10.99.1 とサブネット マスク 255.255.255.255 を持つホストが、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例を示します。

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

次に、任意のホストが、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例を示します。

```
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の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ことを指定します。
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の WebVPN 接続上で 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 webvpn コンフィギュレーション モードおよびユーザ名 webvpn コンフィギュレーション モードで **http-comp** コマンドを使用します。コンフィギュレーションからコマンドを削除して、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**}

構文の説明

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	そのグループまたはユーザに対し圧縮がディセーブルにされるよう指示します。

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	透過	シングル	コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	•	—	•	—	—
ユーザ名 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

WebVPN 接続の場合、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** コマンドによって、グループ ポリシー コンフィギュレーション モードおよびユーザ名 webvpn コンフィギュレーション モードで設定された **http-comp** コマンドが上書きされます。

例

次に、グローバル ポリシー sales の圧縮をディセーブルにする例を示します。

```
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、WebVPN、IPSec VPN 接続で、圧縮をイネーブルにします。

http-proxy

外部プロキシ サーバを使用して HTTP 要求を処理するようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション 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。

http-proxy {*host* [*port*] [**exclude** *url*] | **pac** *pacfile*} [**username** *username* {**password** *password*}]

no http-proxy

構文の説明

host	外部 HTTP プロキシ サーバのホスト名または IP アドレス。
pac *pacfile*	1 つ以上のプロキシを指定する JavaScript 関数を含む PAC ファイルを指定します。
password	（任意。*username* を指定した場合に限り使用可能）各 HTTP プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTP 要求とともにプロキシ サーバに送信されるパスワード。
port	（任意）HTTP プロキシ サーバによって使用されるポート番号。デフォルト ポートは 80 です。値を指定しなかった場合、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。指定できる範囲は 1 ～ 65535 です。
url	プロキシ サーバへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 • [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
username	（任意）各 HTTP プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTP 要求とともにプロキシ サーバに送信されるユーザ名。

デフォルト

デフォルトでは、HTTP プロキシ サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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
8.0(2)	**exclude**、**username**、および **password** のキーワードが追加されました。
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

組織が管理するサーバを経由したインターネットへのアクセスを必須にすると、セキュアなインターネット アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

セキュリティ アプライアンスでサポートされるのは、http-proxy コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての http-proxy コマンドがリストされます。応答に **http-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

例

次の例は、次の設定の HTTP プロキシ サーバの使用を設定する方法を示しています。IP アドレスが 209.165.201.2 のデフォルト ポート（443）を使用。

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 209.165.201.2
hostname(config-webvpn)
```

次に、同じプロキシ サーバを使用して、各 HTTP 要求とともにユーザ名およびパスワードを送信するように設定する例を示します。

```
hostname(config-webvpn)# http-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、セキュリティ アプライアンスが HTTP 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。

```
hostname(config-webvpn)# http-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)
```

次に、exclude オプションの使用例を示します。

```
hostname(config-webvpn)# http-proxy 10.1.1.1 port 8080 exclude *.com username John pasword
12345678
hostname(config-webvpn)
```

次に、pac オプションを使用する例を示します。

```
hostname(config-webvpn)# http-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
https-proxy	外部プロキシ サーバを使用して HTTPS 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバをすべて含めて表示します。

http-proxy（dap）

HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにするには、dap webvpn コンフィギュレーション モードで **http-proxy** コマンドを使用します。
コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

http-proxy {enable | disable | auto-start}

no http-proxy

構文の説明

auto-start	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルにし、自動的に開始します。
enable/disable	DAP レコードの HTTP プロキシ ポート フォワーディングをイネーブルまたはディセーブルにします。

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	透過	シングル	コンテキスト	システム
DAP 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
8.0(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

セキュリティ アプライアンスは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザ、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、セキュリティ アプライアンスはその値を適用して実行します。たとえば、DAP webvpn モードで HTTP プロキシをディセーブルにすると、セキュリティ アプライアンスはそれ以上値を検索しません。代わりに、**http-proxy** コマンドの **no** 値

を使用すると、属性は DAP レコードには存在しないため、セキュリティ アプライアンスは適用する値を見つけるために、ユーザ名および必要に応じてグローバル ポリシーの AAA 属性に移動して検索します。

例

次に、Finance という名前のダイナミック アクセス ポリシー レコードに対して HTTP プロキシ ポート フォワーディングをイネーブルにする例を示します。

```
hostname (config)# dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# http-proxy enable
hostname(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

http redirect

セキュリティ アプライアンスによる HTTP 接続の HTTPS へのリダイレクトを指定するには、グローバル コンフィギュレーション モードで **http 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** バージョンを使用します。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、このコマンドの **no** バージョンを引数なしで使用します。

http redirect *interface* [*port*]

no http redirect [*interface*]

構文の説明

interface	セキュリティ アプライアンスで HTTP 要求を HTTPS にリダイレクトする必要があるインターフェイスを識別します。
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識別します。HTTP 要求はリッスン後 HTTPS にリダイレクトされます。デフォルトでは、ポート 80 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	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

インターフェイスには、HTTP を許可するアクセス リストが必要です。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

次に、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例を示します。

```
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 サーバへのアクセスで経由するセキュリティ アプライアンスの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の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 アプライアンスの 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*]

no http server enable [*port*]

構文の説明

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

デフォルト

HTTP サーバはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

例

次に、HTTP サーバをイネーブルにする例を示します。

```
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 サーバへのアクセスで経由するセキュリティ アプライアンスの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の証明書による認証を要求します。

コマンド	説明
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ことを指定します。
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

外部プロキシ サーバを使用して HTTPS 要求を処理するようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション 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。

https-proxy {*host* [*port*] [**exclude** *url*] | [**username** *username* {**password** *password*}]

no https-proxy

構文の説明

host	外部 HTTPS プロキシ サーバのホスト名または IP アドレス。
password	（任意。*username* を指定した場合に限り使用可能）各 HTTPS プロキシ要求にパスワードを付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
password	各 HTTPS 要求とともにプロキシ サーバに送信されるパスワード。
port	（任意）HTTPS プロキシ サーバによって使用されるポート番号。デフォルト ポートは 443 です。値を指定しなかった場合、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。指定できる範囲は 1 ～ 65535 です。
url	プロキシ サーバへの送信が可能な URL から除外する URL を 1 つ、または複数の URL のカンマ区切りのリストを入力します。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。 • ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字ストリングとともに使用する必要があります。 • **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。 • [*x*-*y*] は、*x* から *y* の範囲にある任意の 1 文字に一致します。ここで、*x* は ANSI 文字セット内の 1 文字を、*y* は ANSI 文字セット内の別の 1 文字を示します。 • [**!***x*-*y*] は、この範囲内に存在しない任意の 1 文字に一致します。
username	（任意）各 HTTPS プロキシ要求にユーザ名を付加して基本的なプロキシ認証を提供するには、このキーワードを入力します。
username	各 HTTPS 要求とともにプロキシ サーバに送信されるユーザ名。

デフォルト

デフォルトでは、HTTPS プロキシ サーバは設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
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
7.3(0)	**exclude**、**username**、および **password** のキーワードが追加されました。
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

組織が管理するサーバを経由したインターネットへのアクセスを必須にすると、セキュアなインターネット アクセスを確保して管理面の制御を保証するためのフィルタリング導入の別のきっかけにもなります。

セキュリティ アプライアンスでサポートされるのは、https-proxy コマンドの 1 つのインスタンスだけです。このコマンドのインスタンスが実行コンフィギュレーションにすでに 1 つ存在する場合、もう 1 つインスタンスを入力すると、CLI は以前のインスタンスを上書きします。**show running-config webvpn** コマンドを入力すると、CLI によって実行コンフィギュレーション内のすべての https-proxy コマンドがリストされます。応答に **https-proxy** コマンドがリストされていない場合、このコマンドは存在しません。

例

次の例は、次の設定の HTTPS プロキシ サーバの使用を設定する方法を示しています：IP アドレスが 209.165.201.2 のデフォルト ポート（443）を使用。

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 209.165.201.2
hostname(config-webvpn)
```

次に、同じプロキシ サーバを使用して、各 HTTPS 要求とともにユーザ名およびパスワードを送信するように設定する例を示します。

```
hostname(config-webvpn)# https-proxy 209.165.201.2 jsmith password mysecretdonttell
hostname(config-webvpn)
```

次も、同じコマンドの例を示しますが、前の例とは異なり、この例では、セキュリティ アプライアンスが HTTPS 要求で www.example.com という特定の URL を受信した場合には、プロキシ サーバに渡すのではなく自分自身で要求を解決します。

```
hostname(config-webvpn)# https-proxy 209.165.201.2 exclude www.example.com username jsmith
password mysecretdonttell
hostname(config-webvpn)

hostname(config-webvpn)# https-proxy 10.1.1.1 port 8080 exclude *.com username John
pasword 12345678
hostname(config-webvpn)
```

次に、pac オプションを使用する例を示します。

```
hostname(config-webvpn)# https-proxy pac http://10.1.1.1/pac.js
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
http-proxy	外部プロキシ サーバを使用して HTTP 要求を処理するように設定します。
show running-config webvpn	SSL VPN の実行コンフィギュレーションを、HTTP および HTTPS のプロキシ サーバをすべて含めて表示します。

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

構文の説明

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

次の表に、コマンドを入力できるモードを示します。

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
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

このコマンドは、ハードウェア モジュールがアップ状態で、パスワード リセットがサポートされている場合にのみ有効です。AIP SSM でこのコマンドを実行すると、モジュールのリブートが発生します。モジュールは、リブートが完了するまで、オフライン状態になります。これには数分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モニタできます。

コマンドは、必ずプロンプトで確認を要求します。コマンドが成功した場合は、それ以上何も出力されません。コマンドが失敗した場合は、障害が発生した理由を示すエラー メッセージが表示されます。表示される可能性のあるエラー メッセージは、次のとおりです。

```
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

次に、スロット 1 のハードウェア モジュールのパスワードをリセットする例を示します。

```
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てリセットします。
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準備をして、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（AIP SSM など）にリカバリ ソフトウェア イメージをロードしたり、TFTP サーバにアクセスするためのネットワーク設定を行ったりするには、特権 EXEC モードで **hw-module module recover** コマンドを使用します。たとえば、SSM で論理イメージをロードできない場合には、このコマンドを使用して SSM を回復する必要があります。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*]}

構文の説明

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** 設定に従ってリカバリ イメージをダウンロードします。ダウンロード後、SSM は新しいイメージからリブートします。
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** キーワードの後にネットワーク パラメータを何も入力しなかった場合、入力を求めるプロンプトが表示されます。
gateway *gateway_ip_address*	（任意）SSM 管理インターフェイスを介して 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*	（任意）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起動します。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。この期間が経過した後で **stop** コマンドを入力すると、SSM が無応答になるなど、予期しない結果になることがあります。
url *tfp_url*	（任意）TFTP サーバ上のイメージの URL。次の形式で指定します。 **tftp:**//*server*/[*path*/]*filename*
vlan *vlan_id*	（任意）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	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

このコマンドは、SSM がアップ、ダウン、無応答、または回復のいずれかの状態である場合にのみ使用可能です。ステート情報については、**show module** コマンドを参照してください。

例

次に、TFTP サーバからイメージをダウンロードするように SSM を設定する例を示します。

```
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
```

次に、SSM を回復する例を示します。

```
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準備をして、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（AIP SSM など）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）には使用できません。

hw-module module 1 reload

構文の説明

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	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

このコマンドは、SSM ステータスがアップである場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

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

例

次に、スロット 1 の SSM をリロードする例を示します。

```
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。

コマンド	説明
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準備をして、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てリセットするには、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

構文の説明

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	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

このコマンドは、SSM ステータスがアップ、ダウン、無応答、または回復のいずれかの場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

SSM がアップ状態の場合、**hw-module module reset** コマンドによって、リセットの前にソフトウェアをシャットダウンするように要求されます。

インテリジェント SSM（AIP SSM など）は、**hw-module module recover** コマンドを使用することで回復できます。SSM が回復状態になっているときに **hw-module module reset** を入力しても、SSM は回復プロセスを中断しません。**hw-module module reset** コマンドによって、SSM のハードウェア リセットが実行され、ハードウェアのリセット後に SSM リカバリが続行されます。SSM がハングした場合は、リカバリ中に SSM をリセットできます。ハードウェア リセットによって、問題が解決することもあります。

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 リセットは行わない **hw-module module reload** コマンドとは異なります。

例

次に、アップ状態になっているスロット 1 の SSM をリセットする例を示します。

```
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準備をして、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

構文の説明

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	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ことによって、コンフィギュレーション データを失うことなく、安全に SSM の電源を切る準備をします。

このコマンドは、SSM ステータスがアップまたは無応答である場合にのみ有効です。ステート情報については、**show module** コマンドを参照してください。

例

次に、スロット 1 の SSM をシャットダウンする例を示します。

```
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。

コマンド	説明
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。