CHAPTER 13

gateway ～ http-map コマンド

gateway

特定のゲートウェイを管理するコール 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*]

シンタックスの説明

gateway	特定のゲートウェイを管理するコール 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 アドレスを指定します。
group_id	コール エージェント グループの ID を 0 ～ 217483647 の範囲で指定します。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

gateway コマンドを使用すると、特定のゲートウェイを管理するコール エージェント グループを指定できます。ゲートウェイの IP アドレスを指定するには、*ip_address* オプションを使用します。*group_id* オプションは、0 ～ 4294967295 の数値で、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* と一致する必要があります。ゲートウェイは 1 つのグループだけに属すことができます。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 でゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 で 2 つのゲートウェイ 10.10.10.116 および 10.10.10.117 を制御するように設定する例を示します。

```
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 のデバッグ情報を表示できるようにします。
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 モードを開始します。
show mgcp	MGCP の設定およびセッション情報を表示します。

global

NAT（ネットワーク アドレス変換）用にマッピングされた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	マッピング先のアドレスとしてインターフェイスの IP アドレスを使用します。
mapped_ifc	マッピング先の IP アドレス ネットワークに接続されたインターフェイスの名前を指定します。
mapped_ip[**-***mapped_ip*]	マッピング先のインターフェイスを終了するときに、実アドレスに変換するマッピング アドレスを指定します。単一アドレスを指定する場合には、PAT（ポート アドレス変換）を設定します。アドレス範囲を指定する場合には、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している場合には、Network Information Center（NIC）に各グローバル IP アドレスを登録する必要があります。
nat_id	NAT ID の整数を指定します。この ID は、変換する実アドレスに、マッピングしたプールを関連付けるために、**nat** コマンドにより参照されます。 標準 NAT の場合、この整数は 1 ～ 2147483647 です。ポリシー NAT（**nat id access-list**）の場合、この整数は 1 ～ 65535 です。 NAT ID 0 には、**global** コマンド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*	（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* とペアにする場合、ネットワークを指定しません。ホストに割り当てる場合、*mapped_ip* に割り当てたサブネット マスクを指定します。アドレス範囲を設定する場合には、*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、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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

ダイナミック NAT および PAT では、最初に **nat** コマンドを設定し、変換する特定のインターフェイス上の実アドレスを指定します。さらに、別のインターフェイスを終了するときに、別個の **global** コマンドを設定して、マッピング アドレス（PAT の場合は 1 つのアドレス）を指定します。各 **nat** コマンドは、各コマンドに割り当てる番号となる NAT ID の値と比較することにより、**global** コマンドと照合されます。

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 の設定を変更し、既存の変換がタイムアウトしないうちに新しい NAT 情報が使用されるようにする場合は、**clear xlate** コマンドを使用して、変換テーブルを消去できます。ただし、変換テーブルを消去すると、現在のすべての接続が切断されます。

例

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 プールを指定し、さらに NAT プールを使い果たした場合に使用する PAT 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)# 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
```

セキュリティ レベルの低い dmz ネットワーク アドレスを変換して、たとえば、内部ネットワーク（10.1.1.0）と同じネットワーク上にあるように見せかけ、ルーティングを簡素化するには、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、1 つの実アドレスに 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、異なるポートを使用する実アドレスと宛先アドレスのペアを 1 つ指定するには、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	コンフィギュレーションから **global** コマンドを削除します。
nat	変換す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-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する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。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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、デリミタは指定されず、グループ名の解析はディセーブルです。

例

次に、**group-delimiter** コマンドを使用して、グループのデリミタをハッシュ符号（#）に変更する例を示します。

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

関連コマンド

コマンド	説明
show running-config group-delimiter	現在のグループのデリミタ値を表示します。
strip-group	ストリップ グループ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 ユーザに対し、トンネル グループ経由のアクセスだけを許可するには、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 username コンフィギュレーション モードで、**group-lock** 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 **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 ポリシーから値を継承できます。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、ユーザが割り当てたトンネル グループと一致しているかどうかを確認することにより、ユーザを制約します。一致していない場合、FWSM はユーザの接続を許可しません。グループロックを設定しない場合、FWSM は、割り当てられたグループとは関係なく、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	グループロックをヌル値に設定し、グループロックの制約を適用しません。デフォルトまたは指定したグループ ポリシーからのグループロック値の継承を防ぎます。
value *tunnel-grp-name*	FWSM がユーザに接続するように要求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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

例

次に、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-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。文字、数字、「_」、「-」、および「.」を任意に組み合わせることができます。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
プロトコル、ネットワーク、サービス、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
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

オブジェクト グループとなるオブジェクトを定義するには、**group-object** コマンドと **object-group** コマンドを併用します。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 モードでこのコマンドを実行します。このコマンドにより、同じタイプのオブジェクトの論理グループを作成し、構造型コンフィギュレーションに階層型オブジェクト グループを構築できます。

オブジェクトがグループ オブジェクトの場合には、オブジェクト グループ内でオブジェクトを重複できます。たとえば、グループ A およびグループ B の両方にオブジェクト 1 が含まれている場合、A および 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する原因となるグループ 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 が含まれている場合、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、ホストの重複設定を不要にする例を示します。

```
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	コンフィギュレーションから、すべての **object-group** コマンドを削除します。
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	設定を最適化するオブジェクト 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*

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、FWSM が属性を問い合わせる AAA サーバ グループを指定します。
from *group-policy_name*	内部グループ ポリシーの属性を、既存グループ ポリシーの値に初期設定します。
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。
password *server_password*	外部 AAA サーバ グループから属性を取得するときに使用するパスワードを指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

FWSM には、[DefaultGroupPolicy] という名前のデフォルトのグループ ポリシーが存在します。ただし、デフォルト 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 FWSM を設定する必要があります。設定方法については、『*Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*』を参照してください。

DefaultGroupPolicy には、次の AVP が設定されています。

属性	デフォルト値
wins-server	なし
dns-server	なし
vpn-access-hours	制限なし
vpn-simultaneous-logins	3
vpn-idle-timeout	30 分
vpn-session-timeout	なし

属性	デフォルト値
vpn-filter	なし
vpn-tunnel-protocol	IPSec WebVPN
ip-comp	ディセーブル
re-xauth	ディセーブル
group-lock	なし
pfs	ディセーブル
client-access-rules	なし
banner	なし
password-storage	ディセーブル
ipsec-udp	ディセーブル
ipsec-udp-port	10000
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	なし
default-domain	なし
split-dns	なし
client-firewall	なし
secure-unit-authentication	ディセーブル
user-authentication	ディセーブル
user-authentication-idle-timeout	なし
ip-phone-bypass	ディセーブル
leap-bypass	ディセーブル
nem	ディセーブル

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 グループに BostonAAA、パスワードに 12345678 を指定し、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 ポリシーの設定を削除します。
group-policy attributes	グループポリシー属性モードを開始し、指定されたグループ ポリシーの AVP を設定できるようにします。
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。

group-policy attributes

グループ ポリシー属性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** 形式を使用します。この属性モードで、指定したグループ ポリシーの AVP を設定できます。

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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

属性モードにおけるこのコマンドの構文には、一般に次の特徴があります。

- **no** 形式を使用すると、実行コンフィギュレーションから属性が削除され、他のグループ ポリシーからの値の継承がイネーブルになります。
- **none** キーワードを使用すると、実行コンフィギュレーションの属性がヌル値に設定され、値は継承されません。
- ブール属性には、イネーブル化およびディセーブル化された設定用の明示的な構文があります。

例

次に、FirstGroup というグループ ポリシーについて、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 ポリシーの設定を削除します。
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。

h225-map

H.225 アプリケーション検査マップを定義するには、グローバル コンフィギュレーション モードで、**h225-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

h225-map *map_name*

no h225-map *map_name*

シンタックスの説明

map_name	H.225 マップの名前を指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
FWSM 3.1	このコマンドが追加されました。

使用上のガイドライン

H.225 マップにより、H.225 コール シグナリングに HSI が含まれている場合、FWSM で H.245 接続用のダイナミックなポート単位のピンホールをオープンできます。

. H.225 マップは、HSI および関連するエンドポイントの情報を提供します。これらは、FWSM によって保護されているネットワークのセキュリティを損なわずに接続を確立するために必要な情報です。

h225-map コマンドを入力すると、特定のマップを定義するための各種コマンドを入力できる、H.225 マップ コンフィギュレーション モードが開始されます。

1 つの H.225 マップに、最大 5 つの HSI グループを含めることができます。各 HSI グループに、最大 10 のエンドポイントを設定できます。

例

次に、H.225 マップを定義する例を示します。

```
hostname(config)# h225-map sample_map
hostname(config-h225-map)# hsi-group 1
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
hostname(config-h225-map-hsi-grp)# exit
```

関連コマンド

コマンド	説明
endpoint	HSI グループに関連付けるエンドポイントを定義します。
hsi	HSI グループに関連付ける HSI を定義します。
hsi-group	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 モードをイネーブルにします。
inspect h323 h225	H.323 アプリケーション検査に H.225 マップを適用します。

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（コマンドライン インターフェイス）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

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

help コマンドは、すべてのコマンドに関するヘルプ情報を表示します。各コマンドのヘルプを表示するには、***help*** コマンドのあとにコマンド名を入力します。コマンド名を指定せずに、***?*** を入力すると、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が表示されます。

pager コマンドをイネーブルにすると、24 行が表示されたあと出力が停止し、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 **more** コマンドと類似した構文を使用します。

- 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*** コマンドのヘルプ情報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、ヘルプ情報を表示する例を示します。

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

コマンド プロンプトに **?** を入力すると、メイン コマンド（**show**、**no**、または **clear** コマンドでない）に関するヘルプ情報が表示されます。

```
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。

hostname

FWSM 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する場合、ホスト名はコマンドを入力したデバイスを追跡するのに役立ちます。

hostname *name*

no hostname [*name*]

シンタックスの説明

name	最大 63 文字でホスト名を指定します。ホスト名の最初と最後は文字または数字で、中間は文字、数字、またはハイフンで構成する必要があります。

デフォルト

デフォルトは、FWSM です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、システムの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 プロンプトに表示されます。

コンテキスト内で任意に設定するホスト名は、コマンドラインには表示されませんが、**banner** コマンドの **$(hostname)** トークンに使用できます。

例

次に、ホスト名を firewall 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、message of the day 、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

HSI に HSI グループを関連付けるには、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。HSI を削除するには、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	HSI の IP アドレスを指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

使用上のガイドライン

HSI グループにより、Cisco CallManager が H.323 エンドポイント間の接続を試みる場合、FWSM で H.323 接続を可能にするダイナミックなポート単位のピンホールをオープンできます。

1 つの H.225 マップに、最大 5 の HSI グループを関連付けることができます。各 HSI グループに、最大 10 のエンドポイントを設定できます。

例

次に、H.225 マップを定義する例を示します。

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
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
hostname(config-h225-map-hsi-grp)# exit
```

関連コマンド

コマンド	説明
endpoint	HSI グループに関連付けるエンドポイントを定義します。
hsi-group	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 モードをイネーブルにします。
h225-map	H.225 マップを定義し、H.225 マップ コンフィギュレーション モードを開始します。
inspect h323 h225	H.323 アプリケーション検査に H.225 マップを適用します。

hsi-group

HSI グループを定義するには、H.225 マップ 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。HSI 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。

hsi-group *group_ID*

no hsi-group *group_*ID

シンタックスの説明

group_name	HSI グループを識別する番号を、0 ～ 2147483647 の範囲で指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
H.225 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
FWSM 3.1	このコマンドが追加されました。

使用上のガイドライン

hsi-group コマンドを入力すると、特定のマップを定義するための各種コマンドを入力できる、HSI グループ コンフィギュレーション モードが開始されます。

HSI グループにより、H.225 コール シグナリングに HSI が含まれている場合、FWSM で H.245 接続用のダイナミックなポート単位のピンホールをオープンできます。

1 つの H.225 マップに、最大 5 の HSI グループを関連付けることができます。各 HSI グループに、最大 10 のエンドポイントを設定できます。エンドポイントを設定する前に、グループ内に HSI を設定しておく必要があります。HSI グループを削除する場合には、事前にすべてのエンドポイントと HSI を削除する必要があります。

例

次に、H.225 マップを定義する例を示します。

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
hostname(config-h225-map-hsi-grp)# hsi 192.168.100.1
hostname(config-h225-map-hsi-grp)# endpoint 192.168.100.101
hostname(config-h225-map-hsi-grp)# endpoint 192.168.100.102
hostname(config-h225-map-hsi-grp)# exit
hostname(config-h225-map)# hsi-group 2
hostname(config-h225-map-hsi-grp)# hsi 192.168.200.1
hostname(config-h225-map-hsi-grp)# endpoint 192.168.200.101
hostname(config-h225-map-hsi-grp)# endpoint 192.168.200.102
hostname(config-h225-map-hsi-grp)# exit
```

関連コマンド

コマンド	説明
endpoint	HSI グループに関連付けるエンドポイントを定義します。
hsi	HSI グループに関連付ける HSI を定義します。
h225-map	H.225 マップを定義し、H.225 マップ コンフィギュレーション モードを開始します。
inspect h323 h225	H.323 アプリケーション検査に H.225 マップを適用します。

hsi-group

HSI グループを定義するには、H.225 マップ 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。HSI 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。

hsi-group *group_ID*

no hsi-group *group_*ID

シンタックスの説明

group_name	HSI グループを識別する番号を、0 ～ 2147483647 の範囲で指定します。

デフォルト

このコマンドには、デフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
H.225 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
FWSM 3.1	このコマンドが追加されました。

使用上のガイドライン

hsi-group コマンドを入力すると、特定のマップを定義するための各種コマンドを入力できる、HSI グループ コンフィギュレーション モードが開始されます。

HSI グループにより、H.225 コール シグナリングに HSI が含まれている場合、FWSM で H.245 接続用のダイナミックなポート単位のピンホールをオープンできます。

1 つの H.225 マップに、最大 5 の HSI グループを関連付けることができます。各 HSI グループに、最大 10 のエンドポイントを設定できます。エンドポイントを設定する前に、グループ内に HSI を設定しておく必要があります。HSI グループを削除する場合には、事前にすべてのエンドポイントと HSI を削除する必要があります。

例

次に、H.225 マップを定義する例を示します。

```
hostname(config)# h225-map hmap
hostname(config-h225-map)# hsi-group 1
hostname(config-h225-map-hsi-grp)# hsi 192.168.100.1
hostname(config-h225-map-hsi-grp)# endpoint 192.168.100.101
hostname(config-h225-map-hsi-grp)# endpoint 192.168.100.102
hostname(config-h225-map-hsi-grp)# exit
hostname(config-h225-map)# hsi-group 2
hostname(config-h225-map-hsi-grp)# hsi 192.168.200.1
hostname(config-h225-map-hsi-grp)# endpoint 192.168.200.101
hostname(config-h225-map-hsi-grp)# endpoint 192.168.200.102
hostname(config-h225-map-hsi-grp)# exit
```

関連コマンド

コマンド	説明
endpoint	HSI グループに関連付けるエンドポイントを定義します。
hsi	HSI グループに関連付ける HSI を定義します。
h225-map	H.225 マップを定義し、H.225 マップ コンフィギュレーション モードを開始します。
inspect h323 h225	H.323 アプリケーション検査に H.225 マップを適用します。

http

FWSM の内部 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。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、引数を指定しないで使用します。

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 サーバにアクセスできる FWSM 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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、IP アドレス 10.10.99.1、サブネット マスク 255.255.255.255 のホストに、外部インターフェイスを経由した HTTP サーバへのアクセスを許可する例を示します。

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

次に、すべてのホストに外部インターフェイスを経由した HTTP サーバへのアクセスを許可する例を示します。

```
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 の設定を削除します。HTTP サーバがディセーブルになり、HTTP サーバにアクセスできるホストが削除されます。
http authentication-certificate	FWSM との HTTPS 接続を確立しているユーザからの証明書を介して、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 サーバがイネーブルであるかどうかに関係なく、HTTP サーバにアクセスできるホストを表示します。

http authentication-certificate

HTTPS 接続を確立するユーザに対して、証明書を使用した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。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。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、このコマンドの **no** 形式を、引数を指定しないで使用します。

FWSM は、PKI トラストポイントと比較して証明書を検証します。証明書が検証に合格しない場合、FWSM は SSL 接続を終了します。

http authentication-certificate *interface*

no http authentication-certificate [*interface*]

シンタックスの説明

interface	証明書による認証を必要とする FWSM 上のインターフェイスを指定します。

デフォルト

HTTP の証明書認証はディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドのサポートが追加されました。

使用上のガイドライン

信頼できる内部インターフェイス上の接続の場合には証明書を提供しなくても済むように、証明書による認証は、インターフェイス単位で設定できます。このコマンドを複数回使用することにより、複数のインターフェイス上に証明書による認証を設定できます。

検証は URL が判別される前に実行されるので、WebVPN および 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。したがって、証明書認証が設定されている場合には、証明書認証およびユーザ名とパスワードの両方が要求されます。証明書認証がディセーブルの場合は、ユーザ名とパスワード認証だけが要求されます。

例

次に、outside および external というインターフェイスに接続するクライアントに対して、証明書による認証を要求する例を示します。

```
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 の設定を削除します。HTTP サーバがディセーブルになり、HTTP サーバにアクセスできるホストが削除されます。
http	IP アドレスおよびサブネット マスクを使用して HTTP サーバにアクセスできるホストを指定します。また、ホストが HTTP サーバにアクセスできる FWSM インターフェイスを指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバがイネーブルであるかどうかに関係なく、HTTP サーバにアクセスできるホストを表示します。

http server enable

FWSM の ASDM 用 HTTPS 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。HTTPS 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

no http server enable

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	トランスペアレント	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更
1.1(1)	このコマンドが追加されました。

例

次に、HTTPS 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 の設定を削除します。HTTP サーバがディセーブルになり、HTTPS サーバにアクセスできるホストが削除されます。
http	IP アドレスおよびサブネット マスクを使用して HTTPS サーバにアクセスできるホストを指定します。また、ホストが HTTPS サーバにアクセスするための FWSM インターフェイスを指定します。
http authentication-certificate	FWSM との HTTPS 接続を確立しているユーザからの証明書を介して、認証を要求します。
show running-config http	HTTPS サーバにアクセス可能なホストのほか、HTTPS サーバがイネーブルにされているか否かを表示します。

http-map

拡張 HTTP 検査パラメータに適用する HTTP マップを作成するには、グローバル コンフィギュレーション モードで、**http-map** コマンドを使用します。この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。

http-map *map_name*

no http-map *map_name*

シンタックスの説明

map_name	HTTP マップの名前を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更
3.1(1)	このコマンドが追加されました。

使用上のガイドライン

拡張 HTTP 検査機能は、アプリケーション ファイアウォールとも呼ばれ、HTTP メッセージが RFC 2616 に適合し、RFC に定義されたサポート対象の拡張方式を使用し、その他の各種条件を満たしているかどうかを検証します。これにより、HTTP メッセージを使用して、ネットワークのセキュリティ ポリシーを回避しようとする攻撃者を防ぐことができます。

（注） HTTP マップを使用して HTTP 検査をイネーブルにすると、動作のリセットとログを伴う厳密な HTTP 検査がデフォルトでイネーブルになります。検査に失敗した場合に実行される動作は変更できますが、HTTP マップがイネーブルである限り、厳密な検査をディセーブルにすることはできません。

ほとんどの場合、条件、および条件を満たしていない場合の FWSM の応答方法を設定できます。HTTP メッセージに適用できる条件は、次のとおりです。

- 設定可能なリストに、いかなる方式も含まれていない
- メッセージのボディ サイズが、設定可能な制限の範囲内である
- 要求および応答メッセージのヘッダー サイズが、設定可能な制限の範囲内である
- URI の長さが、設定可能な制限の範囲内である
- メッセージ ボディのコンテンツ タイプが、ヘッダーと一致している
- 応答メッセージのコンテンツ タイプが、要求 メッセージの accept-type フィールドと一致している

- メッセージのコンテンツ タイプが、事前定義された内部リストに含まれている
- メッセージが HTTP RFC 形式の条件に適合している
- 選択したサポート対象アプリケーションが存在する、または存在しない
- 選択したコード化タイプが存在する、または存在しない

（注）　条件を満たしていないメッセージに指定できる動作は、**allow**、**reset**、または **drop** などの各種コンフィギュレーション コマンドを使用して設定します。これらの動作のほかに、イベントをロギングするかどうかを指定できます。

表 13-1 に、HTTP マップ コンフィギュレーション モードで使用できるコンフィギュレーション コマンドの概要を示します。コマンドの詳細な構文は、このマニュアルの各コマンド エントリを参照してください。

表 13-1　HTTP マップ コンフィギュレーション コマンド

コマンド	説明
content-length	HTTP コンテンツの長さに基づく検査をイネーブルにします。
content-type-verification	HTTP コンテンツのタイプに基づく検査をイネーブルにします。
max-header-length	HTTP ヘッダーの長さに基づく検査をイネーブルにします。
max-uri-length	URI の長さに基づく検査をイネーブルにします。
port-misuse	ポート誤使用のアプリケーション検査をイネーブルにします。
request-method	HTTP 要求方式に基づく検査をイネーブルにします。
strict-http	厳密な HTTP 検査をイネーブルにします。
transfer-encoding	転送コード化タイプに基づく検査をイネーブルにします。

例

次に、HTTP トラフィックを指定し、HTTP マップを定義し、ポリシーを定義し、ポリシーを外部インターフェイスに適用する例を示します。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、FWSM は、以下を含むトラフィックを検出した場合、接続をリセットして、Syslog エントリを作成します。

- 100 バイト未満または 2000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI（ユニフォーム リソース識別子）

関連コマンド

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