CHAPTER 13

# gateway through http-map Commands

# gateway

To specify which group of call agents are managing a particular gateway, use the **gateway** command in MGCP map configuration mode. To remove the configuration, use the **no** form of this command.

**gateway** *ip_address* [*group_id*]

## Syntax Description

| | |
|---|---|
| **gateway** | Specifies the group of call agents that are managing a particular gateway. |
| *group_id* | The ID of the call agent group, from 0 to 2147483647. |
| *ip_address* | The IP address of the gateway. |

## Defaults

This command is disabled by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Mgcp map configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

Use the **gateway** command to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the *ip_address* option. The *group_id* option is a number from 0 to 4294967295 that must correspond with the *group_id* of the call agents that are managing the gateway. A gateway may only belong to one group.

## Examples

The following example allows call agents 10.10.11.5 and 10.10.11.6 to control gateway 10.10.10.115, and allows call agents 10.10.11.7 and 10.10.11.8 to control both gateways 10.10.10.116 and 10.10.10.117:

```
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
```

**Related Commands**

| Commands | Description |
|---|---|
| **debug mgcp** | Enables the display of debug information for MGCP. |
| **mgcp-map** | Defines an MGCP map and enables mgcp map configuration mode. |
| **show mgcp** | Displays MGCP configuration and session information. |

# global

To create a pool of mapped addresses for NAT, use the **global** command in global configuration mode. To remove the pool of addresses, use the **no** form of this command.

**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**}

## Syntax Description

| | |
|---|---|
| **interface** | Uses the interface IP address as the mapped address. |
| *mapped_ifc* | Specifies the name of the interface connected to the mapped IP address network. |
| *mapped_ip*[**-***mapped_ip*] | Specifies the mapped address(es) to which you want to translate the real addresses when they exit the mapped interface. If you specify a single address, then you configure PAT. If you specify a range of addresses, then you configure dynamic NAT.<br><br>If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC). |
| *nat_id* | Specifies an integer for the NAT ID. This ID is referenced by the **nat** command to associate a mapped pool with the real addresses to translate.<br><br>For regular NAT, this integer is between 1 and 2147483647. For policy NAT (**nat id access-list**), this integer is between 1 and 65535.<br><br>Do not specify a **global** command for NAT ID 0; 0 is reserved for identity NAT and NAT exemption, which do not use a **global** command. |
| **netmask** *mask* | (Optional) Specifies the network mask for the *mapped_ip*. This mask does not specify a network when paired with the *mapped_ip*; rather, it specifies the subnet mask assigned to the *mapped_ip* when it is assigned to a host. If you want to configure a range of addresses, you need to specify *mapped_ip***-***mapped_ip*.<br><br>If you do not specify a mask, then the default mask for the address class is used. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |
| 3.2.(1) | NAT is now supported in transparent firewall mode. |

## Usage Guidelines

For dynamic NAT and PAT, you first configure a **nat** command identifying the real addresses on a given interface that you want to translate. Then you configure a separate **global** command to specify the mapped addresses when exiting another interface (in the case of PAT, this is one address). Each **nat** command matches a **global** command by comparing the NAT ID, a number that you assign to each command.

See the **nat** command for more information about dynamic NAT and PAT.

If you change the NAT configuration, and you do not want to wait for existing translations to time out before the new NAT information is used, you can clear the translation table using **clear xlate** command. However, clearing the translation table disconnects all of the current connections.

## Examples

The following example hows how to translate the 10.1.1.0/24 network on the inside interface:

```
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
```

To identify a pool of addresses for dynamic NAT as well as a PAT address for when the NAT pool is exhausted, enter the following commands:

```
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
```

To translate the lower security DMZ network addresses so they appear to be on the same network as the inside network (10.1.1.0), for example, to simplify routing, enter the following commands:

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

To identify a single real address with two different destination addresses using policy NAT, enter the following commands:

```
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
```

To identify a single real address/destination address pair that use different ports using policy NAT, enter the following commands:

```
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
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure global** | Removes **global** commands from the configuration. |
| **nat** | Specifies the real addresses to translate. |
| **show running-config global** | Displays the **global** commands in the configuration. |
| **static** | Configures a one-to-one translation. |

# group-delimiter

To enable group-name parsing and specify the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated, use the **group-delimiter** command in global configuration mode. To disable this group-name parsing, use the no form of this command.

**group-delimiter** *delimiter*

**no group-delimiter**

## Syntax Description

| | |
|---|---|
| *delimiter* | Specifies the character to use as the group-name delimiter. Valid values are: @, #, and !. |

## Defaults

No default behaviors or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | — | — | • |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

By default, no delimiter is specified, disabling group-name parsing.

## Examples

The following example shows the **group-delimiter** command to change the group delimiter to the hash mark (#):

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

## Related Commands

| Command | Description |
|---|---|
| **show running-config group-delimiter** | Displays the current group-delimiter value. |
| **strip-group** | Enables or disables strip-group processing. |

# group-lock

To restrict remote users to access through the tunnel group only, use the **group-lock** command in group-policy configuration mode or username configuration mode. To remove the **group-lock** attribute from the running configuration, use the **no** form of this command.

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

**no group-lock**

## Syntax Description

| | |
|---|---|
| **none** | Sets group-lock to a null value, thereby allowing no group-lock restriction. Prevents inheriting a group-lock value from a default or specified group policy. |
| **value** *tunnel-grp-name* | Specifies the name of an existing tunnel group that the FWSM requires for the user to connect. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Group-policy configuration | • | — | • | — | — |
| Username configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

This option allows inheritance of a value from another group policy. To disable group-lock, use the **group-lock none** command.

Group-lock restricts users by checking if the group configured in the VPN client is the same as the tunnel group to which the user is assigned. If it is not, the FWSM prevents the user from connecting. If you do not configure group-lock, the FWSM authenticates users without regard to the assigned group.

## Examples

The following example shows how to set group lock for the group policy named FirstGroup:

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

This option allows inheritance of a value from another group policy. To disable group-lock, use the **group-lock none** command.

Group-lock restricts users by checking if the group configured in the VPN client is the same as the tunnel group to which the user is assigned. If it is not, the FWSM prevents the user from connecting. If you do not configure group-lock, the FWSM authenticates users without regard to the assigned group.

# group-object

To add network object groups, use the **group-object** command in protocol, network, service, and icmp-type configuration modes. To remove network object groups, use the **no** form of this command.

**group-object** *obj_grp_id*

**no group-object** *obj_grp_id*

## Syntax Description

| | |
|---|---|
| *obj_grp_id* | Identifies the object group (one to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Protocol configuration | • | • | • | • | — |
| Network configuration | • | • | • | • | — |
| Service configuration | • | • | • | • | — |
| Icmp-type configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

The **group-object** command is used with the **object-group** command to define an object that itself is an object group. It is used in protocol, network, service, and icmp-type configuration modes. This command allows logical grouping of the same type of objects and construction of hierarchical object groups for structured configuration.

Duplicate objects are allowed in an object group if they are group objects. For example, if object 1 is in both group A and group B, it is allowed to define a group C which includes both A and B. It is not allowed, however, to include a group object which causes the group hierarchy to become circular. For example, it is not allowed to have group A include group B and then also have group B include group A.

The maximum allowed levels of a hierarchical object group is 10.

## Examples

The following example shows how to use the **group-object** command in network configuration mode eliminate the need to duplicate hosts:

```
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
```

## Related Commands

| Command | Description |
|---|---|
| **clear configure object-group** | Removes all the **object-group** commands from the configuration. |
| **network-object** | Adds a network object to a network object group. |
| **object-group** | Defines object groups to optimize your configuration. |
| **port-object** | Adds a port object to a service object group. |
| **show running-config object-group** | Displays the current object groups. |

# group-policy

To create or edit a group policy, use the **group-policy** command in global configuration mode. To remove a group policy from the configuration, use the **no** form of this command.

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

**no group-policy** *name*

## Syntax Description

| | |
|---|---|
| **external server-group** *server_group* | Specifies the group policy as external and identifies the AAA server group for the FWSM to query for attributes. |
| **from** *group-policy_name* | Initializes the attributes of this internal group policy to the values of a pre-existing group policy. |
| **internal** | Identifies the group policy as internal. |
| *name* | Specifies the name of the group policy. |
| **password** *server_password* | Provides the password to use when retrieving attributes from the external AAA server group. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Global configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

A default group policy, named "DefaultGroupPolicy," always exists on the FWSM. However, this default group policy does not take effect unless you configure the FWSM to use it. For configuration instructions, see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

The DefaultGroupPolicy has these AVPs:

| Attribute | Default Value |
|---|---|
| **wins-server** | none |
| **dns-server** | none |

| Attribute | Default Value |
|---|---|
| **vpn-access-hours** | unrestricted |
| **vpn-simultaneous-logins** | 3 |
| **vpn-idle-timeout** | 30 minutes |
| **vpn-session-timeout** | none |
| **vpn-filter** | none |
| **vpn-tunnel-protocol** | IPSec WebVPN |
| **ip-comp** | disable |
| **re-xauth** | disable |
| **group-lock** | none |
| **pfs** | disable |
| **client-access-rules** | none |
| **banner** | none |
| **password-storage** | disabled |
| **ipsec-udp** | disabled |
| **ipsec-udp-port** | 10000 |
| **backup-servers** | keep-client-config |
| **split-tunnel-policy** | tunnelall |
| **split-tunnel-network-list** | none |
| **default-domain** | none |
| **split-dns** | none |
| **client-firewall** | none |
| **secure-unit-authentication** | disabled |
| **user-authentication** | disabled |
| **user-authentication-idle-timeout** | none |
| **ip-phone-bypass** | disabled |
| **leap-bypass** | disabled |
| **nem** | disabled |

## Examples

The following example shows how to create an internal group policy with the name "FirstGroup":

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

The following example shows how to create an external group policy with the name "ExternalGroup," the AAA server group "BostonAAA," and the password "12345678":

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

## Related Commands

| Command | Description |
|---|---|
| **clear configure group-policy** | Removes the configuration for a particular group policy or for all group policies. |
| **group-policy attributes** | Enters group-policy attributes mode, which lets you configure AVPs for a specified group policy. |
| **show running-config group-policy** | Displays the running configuration for a particular group policy or for all group policies. |

# group-policy attributes

To enter the group-policy attributes mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, user the **no** form of this command. The attributes mode lets you configure AVPs for a specified group policy.

**group-policy** *name* **attributes**

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

## Syntax Description

| | |
|---|---|
| *name* | Specifies the name of the group policy. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

The syntax of the commands in attributes mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration, and enables inheritance of a value from another group policy.
- The **none** keyword sets the attribute in the running configuration to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

## Examples

The following example shows how to enter group-policy attributes mode for the group policy named "FirstGroup":

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

## Related Commands

| Command | Description |
|---|---|
| **clear configure group-policy** | Removes the configuration for a particular group policy or for all group policies. |
| **group-policy** | Creates, edits, or removes a group policy. |
| **show running-config group-policy** | Displays the running configuration for a particular group policy or for all group policies. |

# gtp-map

To identify a specific map to use for defining the parameters for GTP, use the **gtp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

**gtp-map** *map_name*

**no gtp-map** *map_name*

**Note** GTP inspection requires a special license. If you enter the **gtp-map** command on a FWSM without the required license, the FWSM displays an error message.

## Syntax Description

| | |
|---|---|
| *map_name* | The name of the GTP map. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

GPRS is a data network architecture that is designed to integrate with existing GSM networks. It offers mobile subscribers uninterrupted, packet-switched data services to corporate networks and the Internet. For an overview of GTP and how the FWSM ensures secure access over wireless networks, refer to the "Applying Application Layer Protocol Inspection" chapter in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*.

Use the **gtp-map** command to identify a specific map to use for defining the parameters for GTP. When you enter this command, the system enters a configuration mode that lets you enter the different commands used for defining the specific map. After defining the GTP map, you use the **inspect gtp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

*Table 13-1 GTP Map Configuration Commands*

| Command | Description |
|---|---|
| **description** | Specifies the GTP configuration map description. |
| **drop** | Specifies the message ID, APN, or GTP version to drop. |
| **mcc** | Specifies the three-digit Mobile Country Code (000 - 999). One or two- digit entries will be prepended with 0s |
| **message-length** | Specifies the message length min and max. |
| **permit errors** | Permits packets with errors or different GTP versions. |
| **request-queue** | Specifies the maximum requests allowed in the queue. |
| **timeout (gtp-map)** | Specifies the idle timeout for the GSN, PDP context, requests, signaling connections, and tunnels. |
| **tunnel-limit** | Specifies the maximum number of tunnels allowed. |

## Examples

The following example shows how to use the **gtp-map** command to identify a specific map (gtp-policy) to use for defining the parameters for GTP:

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)#
```

The following example shows how to use access lists to identify GTP traffic, define a GTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config-cmap)# match access-list gtp-acl
hostname(config-cmap)# exit
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# request-queue 300
hostname(config-gtpmap)# permit mcc 111 mnc 222
hostname(config-gtpmap)# message-length min 20 max 300
hostname(config-gtpmap)# drop message 20
hostname(config-gtpmap)# tunnel-limit 10000
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy outside
```

## Related Commands

| Commands | Description |
|---|---|
| **class-map** | Defines the traffic class to which to apply security actions. |
| **clear service-policy inspect gtp** | Clears global GTP statistics. |
| **debug gtp** | Displays detailed information about GTP inspection. |
| **inspect gtp** | Applies a specific GTP map to use for application inspection. |
| **show service-policy inspect gtp** | Displays the GTP configuration. |

# h225-map

To define an H.225 application inspection map, use the **h225-map** command in global configuration mode. To remove the map, use the **no** form of this command.

**h225-map** *map_name*

**no h225-map** *map_name*

## Syntax Description

| | |
|---|---|
| *map_name* | The name of the H.225 map. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| FWSM 3.1 | This command was introduced. |

## Usage Guidelines

An H.225 map allows the FWSM to open dynamic, port-specific pinholes for an H.245 connection when an HSI is involved in H.225 call-signalling.

The H.225 map provides information about the HSI and its associated endpoints, which is required to establish this connection without compromising the security of the network protected by the FWSM.

When you enter the **h225-map** command, the system enters the h225 map configuration mode, which lets you enter the different commands used for defining the specific map.

One H.225 map can contain a maximum of five HSI groups. Each HSI group can contain a maximum of ten endpoints.

## Examples

The following example shows how to define an H.225 map:

```
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
```

**Related Commands**

| Commands | Description |
|---|---|
| **endpoint** | Defines the endpoint associated with an HSI group. |
| **hsi** | Defines the HSI associated with an HSI group. |
| **hsi-group** | Defines an HSI group and enables hsi group configuration mode. |
| **inspect h323 h225** | Applies an H.225 map to H.323 application inspection. |

# hello-interval

To specify the interval between EIGRP hello packets sent on an interface, use the **hello-interval** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

**hello-interval eigrp** *as-number seconds*

**no hello-interval eigrp** *as-number seconds*

## Syntax Description

| | |
|---|---|
| *as-number* | The autonomous system number of the EIGRP routing process. |
| *seconds* | Specifies the interval between hello packets that are sent on the interface; valid values are from 1 to 65535 seconds. |

## Defaults

The default *seconds* is 5 seconds.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Interface configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

The smaller the hello interval, the faster topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

## Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

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

## Related Commands

| Command | Description |
|---|---|
| **hold-time** | Configures the EIGRP hold time advertised in hello packets. |

# help

To display help information for the command specified, use the **help** command in user EXEC mode.

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

## Syntax Description

| | |
|---|---|
| *command* | Specifies the command for which to display the CLI help. |
| **?** | Displays all commands that are available in the current privilege level and mode. |

## Defaults

No default behaviors or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| **Command Mode** | **Routed** | **Transparent** | **Single** | **Context** | **System** |
| User EXEC | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

The **help** command displays help information about all commands. You can see help for an individual command by entering the **help** command followed by the command name. If you do not specify a command name and enter **?** instead, all commands that are available in the current privilege level and mode display.

If you enable the **pager** command and when 24 lines display, the listing pauses, and the following prompt appears:

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

The More prompt uses syntax similar to the UNIX **more** command as follows:

- To see another screen of text, press the **Space** bar.
- To see the next line, press the **Enter** key.
- To return to the command line, press the **q** key.

## Examples

The following example shows how to display help for the **rename** command:

```
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#
```

The following examples shows how to display help by entering the command name and a question mark:

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

Help is available for the core commands (not the **show**, **no**, or **clear** commands) by entering **?** at the command prompt:

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

## Related Commands

| Command | Description |
|---|---|
| **show version** | Displays information about the operating system software. |

# hold-time

To specify the hold time advertised by the FWSM in EIGRP hello packets, use the **hold-time** command in interface configuration mode. To return the hello interval to the default value, use the **no** form of this command.

**hold-time eigrp** *as-number seconds*

**no hold-time eigrp** *as-number seconds*

## Syntax Description

| | |
|---|---|
| *as-number* | The autonomous system number of the EIGRP routing process. |
| *seconds* | Specifies the hold time, in seconds. Valid values are from 1 to 65535 seconds. |

## Defaults

`The default *seconds* is 15 seconds.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Interface configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 4.0(1) | This command was introduced. |

## Usage Guidelines

This value is advertised in the EIGRP hello packets sent by the FWSM. The EIGRP neighbors on that interface use this value to determine the availability of the FWSM. If they do not receive a hello packet from the FWSM during the advertised hold time, the EIGRP neighbors will consider the FWSM to be unavailable.

On very congested and large networks, the default hold time might not be sufficient time for all routers and access servers to receive hello packets from their neighbors. In this case, you may want to increase the hold time.

We recommend that the hold time be at least three times the hello interval. If the FWSM does not receive a hello packet within the specified hold time, routes through this neighbor are considered unavailable.

Increasing the hold time delays route convergence across the network.

## Examples

The following example sets the EIGRP hello interval to 10 seconds and the hold time to 30 seconds:

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

**Related Commands**

| Command | Description |
|---|---|
| **hello-interval** | Specifies the interval between EIGRP hello packets sent on an interface. |

# hostname

To set the FWSM hostname, use the **hostname** command in global configuration mode. To restore the default hostname, use the **no** form of this command. The hostname appears as the command line prompt, and if you establish sessions to multiple devices, the hostname helps you keep track of where you enter commands.

**hostname** *name*

**no hostname** [*name*]

## Syntax Description

| | |
|---|---|
| *name* | Specifies a hostname up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen. |

## Defaults

The default is FWSM.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | • |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Usage Guidelines

For multiple context mode, the hostname that you set in the system execution space appears in the command line prompt for all contexts.

The hostname that you optionally set within a context does not appear in the command line, but can be used for the **banner** command **$(hostname)** token.

## Examples

The following example sets the hostname to firewall1:

```
hostname(config)# hostname firewall1
firewall11(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **banner** | Sets a login, message of the day, or enable banner. |
| **domain-name** | Sets the default domain name. |

# hsi

To associate an HSI with an HSI group, use the **hsi** command in hsi group configuration mode. To remove the HSI, use the **no** form of this command.

**hsi** *ip address*

**no hsi** *ip address*

## Syntax Description

| | |
|---|---|
| *ip address* | The IP address of the HSI. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Hsi group configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| FWSM 3.1 | This command was introduced. |

## Usage Guidelines

An HSI group allows the FWSM to open dynamic, port-specific pinholes for enabling H.323 connections when a Cisco CallManager tries to establish a connection between H.323 endpoints.

Up to five HSI groups can be associated with a single H.225 map. Each HSI group can contain a maximum of ten endpoints.

## Examples

The following example shows how to define an H.225 map:

```
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
```

## Related Commands

| Commands | Description |
|---|---|
| **endpoint** | Defines the endpoint associated with an HSI group. |
| **hsi-group** | Defines an HSI group and enables hsi group configuration mode. |

| Commands | Description |
|---|---|
| **h225-map** | Defines an H.225 map and enables h225 map configuration mode. |
| **inspect h323 h225** | Applies an H.225 map to H.323 application inspection. |

# hsi-group

To define an HSI group, use the **hsi-group** command in h225 map configuration mode. To remove the HSI group, use the **no** form of this command.

**hsi-group** *group_ID*

**no hsi-group** *group*_ID

## Syntax Description

| | |
|---|---|
| *group_name* | A number, from 0 to 2147483647, that identifies the HSI group. |

## Defaults

No default behavior or values.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| H.225 map configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| FWSM 3.1 | This command was introduced. |

## Usage Guidelines

When you enter the **hsi-group** command, the system enters the HSI group configuration mode, which lets you enter the different commands used for defining the specific map.

A HSI group allows the FWSM to open dynamic, port-specific pinholes for an H.245 connection when an HSI is involved in H.225 call-signalling.

Up to five HSI groups can be associated with a single H.225 map. Each HSI group can contain a maximum of ten endpoints. You must configure an HSI within the group before configuring any endpoints. You must remove all endpoints and the HSI before removing the HSI group.

## Examples

The following example shows how to define an H.225 map:

```
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
```

## Related Commands

| Commands | Description |
|---|---|
| **endpoint** | Defines the endpoint associated with an HSI group. |
| **hsi** | Defines the HSI associated with an HSI group. |
| **h225-map** | Defines an H.225 map and enables h225 map configuration mode. |
| **inspect h323 h225** | Applies an H.225 map to H.323 application inspection. |

# http

To specify hosts that can access the HTTP server internal to the FWSM, use the **http** command in global configuration mode. To remove one or more hosts, use the **no** form of this command. To remove the attribute from the configuration, use the **no** form of this command without arguments.

**http** *ip_address subnet_mask interface_name*

**no http**

## Syntax Description

| | |
|---|---|
| *interface_name* | Provides the name of the FWSM interface through which the host can access the HTTP server. |
| *ip_address* | Provides the IP address of a host that can access the HTTP server. |
| *subnet_mask* | Provides the subnet mask of a host that can access the HTTP server. |

## Defaults

No hosts can access the HTTP server.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Examples

The following example shows how to allow the host with the IP address of 10.10.99.1 and the subnet mask of 255.255.255.255 access to the HTTP server via the outside interface:

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

The next example shows how to allow any host access to the HTTP server via the outside interface:

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

## Related Commands

| Command | Description |
|---|---|
| **clear configure http** | Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server. |
| **http authentication-certificate** | Requires authentication via certificate from users who are establishing HTTPS connections to the FWSM. |

| Command | Description |
|---|---|
| **http server enable** | Enables the HTTP server. |
| **show running-config http** | Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled. |

# http authentication-certificate

To require authentication via certificate from users who are establishing HTTPS connections, use the **http authentication-certificate** command in global configuration mode. To remove the attribute from the configuration, use the **no** form of this command. To remove all **http authentication-certificate** commands from the configuration, use the **no** form without arguments.

**http authentication-certificate** *interface*

**no http authentication-certificate** [*interface*]

## Syntax Description

| | |
|---|---|
| *interface* | Specifies the interface on the FWSM that requires certificate authentication. |

## Defaults

HTTP certificate authentication is disabled.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | — | • | — | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | Support for this command was introduced. |

## Usage Guidelines

The FWSM validates certificates against the PKI trust points. If a certificate does not pass validation, the FWSM closes the SSL connection.

You can configure certificate authentication for each interface, such that connections on a trusted/inside interface do not have to provide a certificate. You can use the command multiple times to enable certificate authentication on multiple interfaces.

Validation occurs before the URL is known, so this affects both WebVPN and ASDM access.

The ASDM uses its own authentication method in addition to this value. That is, it requires both certificate and username/password authentication if both are configured, or just username/password if certificate authentication is disabled.

## Examples

The following example shows how to require certificate authentication for clients connecting to the interfaces named outside and external:

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

## Related Commands

| Command | Description |
|---|---|
| **clear configure http** | Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server. |
| **http** | Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the FWSM interface through which the host accesses the HTTP server. |
| **http server enable** | Enables the HTTP server. |
| **show running-config http** | Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled. |

# http server enable

To enable the FWSM HTTPS server for ASDM, use the **http server enable** command in global configuration mode. To disable the HTTPS server, use the **no** form of this command.

**http server enable**

**no http server enable**

## Defaults

The HTTP server is disabled.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 1.1(1) | This command was introduced. |

## Examples

The following example shows how to enable the HTTPS server:

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

## Related Commands

| Command | Description |
|---|---|
| **clear configure http** | Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTPS server. |
| **http** | Specifies hosts that can access the HTTPS server by IP address and subnet mask. Specifies the FWSM interface through which the host accesses the HTTPS server. |
| **http authentication-certificate** | Requires authentication via certificate from users who are establishing HTTPS connections to the FWSM. |
| **show running-config http** | Displays the hosts that can access the HTTPS server, and whether or not the HTTPS server is enabled. |

# http-map

To create an HTTP map for applying enhanced HTTP inspection parameters, use the **http-map** command in global configuration mode. To remove the command, use the **no** form of this command.

**http-map** *map_name*

**no http-map** *map_name*

## Syntax Description

| | |
|---|---|
| *map_name* | The name of the HTTP map. |

## Defaults

This command is disabled by default.

## Command Modes

The following table shows the modes in which you can enter the command:

| | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | | | | Multiple | |
| Command Mode | Routed | Transparent | Single | Context | System |
| Global configuration | • | • | • | • | — |

## Command History

| Release | Modification |
|---|---|
| 3.1(1) | This command was introduced. |

## Usage Guidelines

The enhanced HTTP inspection feature, which is also known as an application firewall, verifies that HTTP messages conform to RFC 2616, use RFC-defined and supported extension methods, and comply with various other criteria. This can help prevent attackers from using HTTP messages for circumventing network security policy.

**Note** When you enable HTTP inspection with an HTTP map, strict HTTP inspection with the action reset and log is enabled by default. You can change the actions performed in response to inspection failure, but you cannot disable strict inspection as long as the HTTP map remains enabled.

In many cases, you can configure the criteria and how the FWSM responds when the criteria are not met. The criteria that you can apply to HTTP messages include the following:

- Does not include any method on a configurable list.
- Message body size is within configurable limits.
- Request and response message header size is within a configurable limit.
- URI length is within a configurable limit.
- The content-type in the message body matches the header.
- The content-type in the response message matches the accept-type field in the request message.

- The content-type in the message is included in a predefined internal list.
- Message meets HTTP RFC format criteria.
- Presence or absence of selected supported applications.
- Presence or absence of selected encoding types.

**Note** The actions that you can specify for messages that fail the criteria set using the different configuration commands include **allow**, **reset**, or **drop**. In addition to these actions, you can specify to log the event or not.

Table 13-2 summarizes the configuration commands available in HTTP map configuration mode. For detailed syntax for a command, see the corresponding command entry in this guide.

*Table 13-2 HTTP Map Configuration Commands*

| Command | Description |
|---|---|
| **content-length** | Enables inspection based on the length of the HTTP content. |
| **content-type-verification** | Enables inspection based on the type of HTTP content. |
| **max-header-length** | Enables inspection based on the length of the HTTP header. |
| **max-uri-length** | Enables inspection based on the length of the URI. |
| **port-misuse** | Enables port misuse application inspection. |
| **request-method** | Enables inspection based on the HTTP request method. |
| **strict-http** | Enables strict HTTP inspection. |
| **transfer-encoding** | Enables inspection based on the transfer encoding type. |

## Examples

The following example shows how to identify HTTP traffic, define an HTTP map, define a policy, and apply the policy to the outside interface:

```
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
```

This example causes the FWSM to reset the connection and create a syslog entry when it detects any traffic that contain the following:

- Messages less than 100 bytes or exceeding 2000 bytes
- Unsupported content types
- HTTP headers exceeding 100 bytes

- URIs exceeding 100 bytes

## Related Commands

| Commands | Description |
|---|---|
| **class-map** | Defines the traffic class to which to apply security actions. |
| **debug appfw** | Displays detailed information about HTTP application inspection. |
| **debug http-map** | Displays detailed information about traffic associated with an HTTP map. |
| **inspect http** | Applies a specific HTTP map to use for application inspection. |
| **policy-map** | Associates a class map with specific security actions. |