



## gateway through hw-module module shutdown 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

<b>gateway</b>	Specifies the group of call agents that are managing a particular gateway
<i>ip_address</i>	The IP address of the gateway.
<i>group_id</i>	The ID of the call agent group, from 0 to 2147483647.

## Defaults

This command is disabled by default.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
MGCP map configuration	•	•	•	•	—

## Command History

Release	Modification
7.0(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
	<b>debug mgcp</b>	Enables the display of debug information for MGCP.
	<b>mgcp-map</b>	Defines an MGCP map and enables MGCP map configuration mode.
	<b>show mgcp</b>	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

<b>interface</b>	Uses the interface IP address as the mapped address. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP.
<i>mapped_ifc</i>	Specifies the name of the interface connected to the mapped IP address network.
<i>mapped_ip</i> [- <i>mapped_ip</i> ]	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.  If the external network is connected to the Internet, each global IP address must be registered with the Network Information Center (NIC).
<i>nat_id</i>	Specifies an integer for the NAT ID. This ID is referenced by the <b>nat</b> command to associate a mapped pool with the real addresses to translate.  For regular NAT, this integer is between 1 and 2147483647. For policy NAT ( <b>nat id access-list</b> ), this integer is between 1 and 65535.  Do not specify a <b>global</b> command for NAT ID 0; 0 is reserved for identity NAT and NAT exemption, which do not use a <b>global</b> command.
<b>netmask</b> <i>mask</i>	(Optional) Specifies the network mask for the <i>mapped_ip</i> . This mask does not specify a network when paired with the <i>mapped_ip</i> ; rather, it specifies the subnet mask assigned to the <i>mapped_ip</i> when it is assigned to a host. If you want to configure a range of addresses, you need to specify <i>mapped_ip-mapped_ip</i> .  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:

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

**Command History**

Release	Modification
Preexisting	This command was preexisting.

**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**

For example, to translate the 10.1.1.0/24 network on the inside interface, enter the following command:

```
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**

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

# group-alias

To create one or more alternate names by which the user can refer to a tunnel-group, use the **group-alias** command in tunnel-group webvpn configuration mode. To remove an alias from the list, use the **no** form of this command.

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

**no group-alias** *name*

## Syntax Description

<b>disable</b>	Disables the group alias.
<b>enable</b>	Enables a previously disabled group alias.
<i>name</i>	Specifies the name of a tunnel group alias. This can be any string you choose, except that the string cannot contain spaces.

## Defaults

No default group alias, but if you do specify a group alias, that alias is enabled by default.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

## Command History

Release	Modification
7.1(1)	This command was introduced.

## Usage Guidelines

The group alias that you specify here appears in the drop-down list on the login page. Each group can have multiple aliases or no alias. This command is useful when the same group is known by several common names, such as “Devtest” and “QA”.

## Examples

The following example shows the commands for configuring the webvpn tunnel group named “devtest” and establishing the aliases “QA” and “Fra-QA” for the group:

```
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)#
```

Related Commands	Command	Description
	<b>clear configure tunnel-group</b>	Clears the entire tunnel-group database or the named tunnel group configuration.
	<b>show webvpn group-alias</b>	Displays the aliases for the specified tunnel group or for all tunnel groups.
	<b>tunnel-group webvpn-attributes</b>	Enters the tunnel-group webvpn configuration mode for configuring WebVPN tunnel-group attributes.

# 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

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

## Command Modes

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

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Usage Guidelines

The delimiter is used to parse tunnel group names from user names when tunnels are negotiated.

## Examples

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

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

## Related Commands

Command	Description
<b>clear configure group-delimiter</b>	Clears the configured group delimiter.
<b>show running-config group-delimiter</b>	Displays the current group-delimiter value.
<b>strip-group</b>	Enables or disables strip-group processing.

# group-lock

To restrict remote users to access through the tunnel group only, issue 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. 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 security appliance prevents the user from connecting. If you do not configure group-lock, the security appliance authenticates users without regard to the assigned group.

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

**no group-lock**

## Syntax Description

<b>none</b>	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.
<b>value</b> <i>tunnel-grp-name</i>	Specifies the name of an existing tunnel group that the security appliance 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:

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## 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
```

# 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Protocol, network, service, icmp-type configuration	•	•	•	•	—

## Command History

Release	Modification
Preexisting	This command was preexisting.

## 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 sub-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**

<b>Command</b>	<b>Description</b>
<b>clear configure object-group</b>	Removes all the <b>object-group</b> commands from the configuration.
<b>network-object</b>	Adds a network object to a network object group.
<b>object-group</b>	Defines object groups to optimize your configuration.
<b>port-object</b>	Adds a port object to a service object group.
<b>show running-config object-group</b>	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

<b>external server-group</b> <i>server_group</i>	Specifies the group policy as external and identifies the AAA server group for the security appliance to query for attributes.
<b>from</b> <i>group-policy_name</i>	Initializes the attributes of this internal group policy to the values of a pre-existing group policy.
<b>internal</b>	Identifies the group policy as internal.
<i>name</i>	Specifies the name of the group policy.
<b>password</b> <i>server_password</i>	Provides the password to use when retrieving attributes from the external AAA server group.

## Defaults

No default behavior or values. See Usage Guidelines.

## Command Modes

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

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

## Command History

Release	Modification
7.0.1	This command was introduced.

## Usage Guidelines

A default group policy, named “DefaultGroupPolicy,” always exists on the security appliance. However, this default group policy does not take effect unless you configure the security appliance to use it. For configuration instructions, see the *Cisco Security Appliance Command Line Configuration Guide*.

Use the **group-policy attributes** command to enter config-group-policy mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
<b>backup-servers</b>	keep-client-config
<b>banner</b>	none

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

In addition, you can configure webvpn-mode attributes for the group policy, either by entering the **webvpn** command in config-group-policy mode or by entering the **group-policy attributes** command and then entering the **webvpn** command in config-group-webvpn mode. See the description of the **group-policy attributes** command for details.

### Examples

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

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

The next 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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear configure group-policy</b>	Removes the configuration for a particular group policy or for all group policies.
	<b>group-policy attributes</b>	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn mode to configure webvpn attributes for the group.
	<b>show running-config group-policy</b>	Displays the running configuration for a particular group policy or for all group policies.
	<b>webvpn</b>	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

# group-policy attributes

To enter the config-group-policy mode, use the **group-policy attributes** command in global configuration mode. To remove all attributes from a group policy, use the **no** version of this command. In config-group-policy mode, you can configure Attribute-Value Pairs for a specified group policy or enter group-policy webvpn configuration mode to configure webvpn attributes for the group.

**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:

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

## Command History

Release	Modification
7.0.1	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.

A default group policy, named DefaultGroupPolicy, always exists on the security appliance. However, this default group policy does not take effect unless you configure the security appliance to use it. For configuration instructions, see the *Cisco Security Appliance Command Line Configuration Guide*.

The **group-policy attributes** command enters config-group-policy mode, in which you can configure any of the group-policy Attribute-Value Pairs. The DefaultGroupPolicy has these Attribute-Value Pairs:

Attribute	Default Value
<b>backup-servers</b>	keep-client-config
<b>banner</b>	none

Attribute	Default Value
<b>client-access-rule</b>	none
<b>client-firewall</b>	none
<b>default-domain</b>	none
<b>dns-server</b>	none
<b>group-lock</b>	none
<b>ip-comp</b>	disable
<b>ip-phone-bypass</b>	disabled
<b>ipsec-udp</b>	disabled
<b>ipsec-udp-port</b>	10000
<b>leap-bypass</b>	disabled
<b>nem</b>	disabled
<b>password-storage</b>	disabled
<b>pfs</b>	disable
<b>re-xauth</b>	disable
<b>secure-unit-authentication</b>	disabled
<b>split-dns</b>	none
<b>split-tunnel-network-list</b>	none
<b>split-tunnel-policy</b>	tunnelall
<b>user-authentication</b>	disabled
<b>user-authentication-idle-timeout</b>	none
<b>vpn-access-hours</b>	unrestricted
<b>vpn-filter</b>	none
<b>vpn-idle-timeout</b>	30 minutes
<b>vpn-session-timeout</b>	none
<b>vpn-simultaneous-logins</b>	3
<b>vpn-tunnel-protocol</b>	IPSec WebVPN
<b>wins-server</b>	none

In addition, you can configure webvpn-mode attributes for the group policy, by entering the **group-policy attributes** command and then entering the **webvpn** command in config-group-policy mode. See the description of the **webvpn** command (group-policy attributes and username attributes modes) for details.

### 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

<b>Command</b>	<b>Description</b>
<b>clear configure group-policy</b>	Removes the configuration for a particular group policy or for all group policies.
<b>group-policy</b>	Creates, edits, or removes a group policy.
<b>show running-config group-policy</b>	Displays the running configuration for a particular group policy or for all group policies.
<b>webvpn (group-policy attributes mode)</b>	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

# group-prompt

To customize the group prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **group-prompt** command from webvpn customization mode:

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

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

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

## Syntax Description

<b>text</b>	Specifies you are changing the text.
<b>style</b>	Specifies you are changing the style.
<i>value</i>	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

## Defaults

The default text of the group prompt is “GROUP:”.

The default style of the group prompt is color:black;font-weight:bold;text-align:right.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn customization	•	—	•	—	—

## Command History

Release	Modification
7.1(1)	This command was introduced.

## Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (W3C) website at [www.w3.org](http://www.w3.org). Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at [www.w3.org/TR/CSS21/propidx.html](http://www.w3.org/TR/CSS21/propidx.html).

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.
- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

**Note**

To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

**Examples**

In the following example, the text is changed to “Corporate Group:”, and the default style is changed with the font weight increased to bolder:

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

**Related Commands**

Command	Description
<b>password-prompt</b>	Customizes the password prompt of the WebVPN page.
<b>username-prompt</b>	Customizes the username prompt of the WebVPN page.

## group-url

To specify incoming URLs or IP addresses for the group, use the **group-url** command in tunnel-group webvpn configuration mode. To remove a URL from the list, use the **no** form of this command.

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

```
no group-url url
```

### Syntax Description

<b>disable</b>	Disables the URL, but does not remove it from the list.
<b>enable</b>	Enables the URL.
<i>url</i>	Specifies a URL or IP address for this tunnel group.

### Defaults

There is no default URL or IP address, but if you do specify a URL or IP address, it is enabled by default.

### Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group webvpn configuration	•	—	•	—	—

### Command History

Release	Modification
7.1(1)	This command was introduced.

### Usage Guidelines

Specifying a group URL or IP address eliminates the need for the user to select a group at login. When a user logs in, the security appliance looks for the user's incoming URL/address in the tunnel-group-policy table. If it finds the URL/address and if group-url is enabled in the tunnel group, then the security appliance automatically selects the associated tunnel group and presents the user with only the username and password fields in the login window. This simplifies the user interface and has the added advantage of never exposing the list of groups to the user. The login window that the user sees uses the customizations configured for that tunnel group.

If the URL/address is disabled and group-alias is configured, then the dropdown list of groups is also displayed, and the user must make a selection.

You can configure multiple URLs/addresses (or none) for a group. Each URL/address can be enabled or disabled individually. You must use a separate **group-url** command for each URL/address specified. You must specify the entire URL/address, including either the http or https protocol.

You cannot associate the same URL/address with multiple groups. The security appliance verifies the uniqueness of the URL/address before accepting the URL/address for a tunnel group.

The following example shows the commands for configuring the webvpn tunnel group named “test” and establishing two group URLs, “http://www.cisco.com” and “https://supplier.com” for the group:

```
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.com
hostname(config-tunnel-webvpn)#
```

The following example enables the group URLs http://www.cisco.com and http://192.168.10.10 for the tunnel-group named RadiusServer:

```
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)#
```

#### Related Commands

Command	Description
<b>clear configure tunnel-group</b>	Clears the entire tunnel-group database or the named tunnel group configuration.
<b>show webvpn group-url</b>	Displays the URLs for the specified tunnel group or for all tunnel groups.
<b>tunnel-group webvpn-attributes</b>	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

# 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 security appliance without the required license, the security appliance displays an error message.

## Syntax Description

<i>map_name</i>	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:

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

## Command History

Release	Modification
7.0(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 security appliance ensures secure access over wireless networks, refer to the “Applying Application Layer Protocol Inspection” chapter in the *Cisco Security Appliance Command Line 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
<b>description</b>	Specifies the GTP configuration map description.
<b>drop</b>	Specifies the message ID, APN, or GTP version to drop.
<b>help</b>	Displays help for GTP map configuration commands.
<b>mcc</b>	Specifies the three-digit Mobile Country Code (000 - 999). One or two-digit entries will be prepended with 0s
<b>message-length</b>	Specifies the message length min and max
<b>permit errors</b>	Permits packets with errors or different GTP versions.
<b>request-queue</b>	Specifies the maximum requests allowed in the queue.
<b>timeout (gtp-map)</b>	Specifies the idle timeout for the GSN, PDP context, requests, signaling connections, and tunnels.
<b>tunnel-limit</b>	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 gtp-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
<b>class-map</b>	Defines the traffic class to which to apply security actions.
<b>clear service-policy inspect gtp</b>	Clears global GTP statistics.
<b>debug gtp</b>	Displays detailed information about GTP inspection.
<b>inspect gtp</b>	Applies a specific GTP map to use for application inspection.
<b>show service-policy inspect gtp</b>	Displays the GTP configuration.

# help

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

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

## Syntax Description

<i>command</i>	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:

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

## Command History

Release	Modification
Preexisting	This command was preexisting.

## 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
<a href="#">show version</a>	Displays information about the operating system software.

# hic-fail-group-policy

To specify a group policy to grant a WebVPN user access rights that are different from the default group policy, use the **hic-fail-group-policy** command in tunnel-group-webvpn configuration mode. The **no** form of this command sets the group policy to the default group policy.

**hic-fail-group-policy** *name*

**no hic-fail-group-policy**

## Syntax Description

*name* Specifies the name of the group policy.

## Defaults

DfltGrpPolicy

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group-webvpn configuration	•	—	•	—	—

## Command History

Release	Modification
7.1(1)	This command was introduced.

## Usage Guidelines

This command is valid only for security appliances with Cisco Secure Desktop installed. Host integrity checking, also called *System Detection*, involves checking the remote PC for a minimal set of criteria that must be satisfied to apply a VPN feature policy. The security appliance uses the value of the hic-fail-group-policy attribute to limit access rights to remote CSD users as follows:

- Always uses it if you set the VPN feature policy to “Use Failure Group-Policy.”
- Uses it if you set the VPN feature policy to “Use Success Group-Policy, if criteria match” and the criteria then fail to match.

This attribute specifies the name of the failure group policy to be applied. Use a group policy to differentiate access rights from those associated with the default group policy.



### Note

The security appliance does not use this attribute if you set the VPN feature policy to “Always use Success Group-Policy.”

For more information, see the *Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*.

**Examples**

The following example creates a WebVPN tunnel group named “FirstGroup” and specifies the failure group policy with the name “group2”:

```
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)#
```

**Related Commands**

Command	Description
<b>clear configure group-policy</b>	Removes the configuration for a particular group policy or for all group policies.
<b>show running-config group-policy</b>	Displays the running configuration for a particular group policy or for all group policies.
<b>tunnel-group webvpn-attributes</b>	Specifies the WebVPN attributes for the named tunnel-group.

# hidden-parameter

To specify hidden parameters in the HTTP POST request that the security appliance submits to the authenticating web server for SSO authentication, use the **hidden-parameter** command in aaa-server-host configuration mode.

To remove all hidden parameters from the running configuration, use the **no** form of the command.

This is an SSO with HTTP Forms command.

**hidden-parameter** *string*

**no hidden-parameter**



## Note

To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

## Syntax Description

*string* A hidden parameter embedded in the form and sent to the SSO server. You can enter it on multiple lines. The maximum number of characters for each line is 255. The maximum number of characters for all lines together—the complete hidden parameter—is 2048.

## Defaults

No default value or behavior.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Aaa-server-host configuration	•	—	•	—	—

## Command History

Release	Modification
7.1(1)	This command was introduced.

## Usage Guidelines

The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. That request may require specific hidden parameters from the SSO HTML form—other than username and password—that are not visible to the user. You can discover hidden parameters that the web server expects in the POST request by using a HTTP header analyzer on a form received from the web server.

The command **hidden-parameter** lets you specify a hidden parameter the web server requires in the authentication POST request. If you use a header analyzer, you can copy and paste the whole hidden parameter string including any encoded URL parameters.

For ease of entry, you can enter a hidden parameter on multiple, sequential lines. The security appliance then concatenates the lines into a single hidden parameter. While the maximum characters per hidden-parameter line is 255 characters, you can enter fewer characters on each line.

**Note**

Any question mark in the string must be preceded by a CTRL-v escape sequence.

**Examples**

The following example shows a hidden parameter comprised of four form entries and their values, separated by &. Excerpted from the POST request, the four entries and their values are:

- SMENC with a value of ISO-8859-1
- SMLOCALE with a value of US-EN
- target with a value of `https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG`
- smauthreason with a value of 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)#
```

**Related Commands**

Command	Description
<b>action-uri</b>	Specifies a web server URI to receive a username and password for single sign-on authentication.
<b>auth-cookie-name</b>	Specifies a name for the authentication cookie.
<b>password-parameter</b>	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
<b>start-url</b>	Specifies the URL at which to retrieve a pre-login cookie.
<b>user-parameter</b>	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

# homepage

To specify a URL for the web page that displays upon login for this WebVPN user or group policy, use the **homepage** command in webvpn mode, which you enter from group-policy or username mode. To remove a configured home page, including a null value created by issuing the **homepage none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a home page, use the **homepage none** command.

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

**no homepage**

## Syntax Description

<b>none</b>	Indicates that there is no WebVPN home page. Sets a null value, thereby disallowing a home page. Prevents inheriting an home page.
<b>value</b> <i>url-string</i>	Provides a URL for the home page. The string must begin with either http:// or https://.

## Defaults

There is no default home page.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn mode	•	—	•	—	—

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Examples

The following example shows how to specify www.example.com as the home page for the group policy named FirstGroup:

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

## Related Commands

Command	Description
<b>webvpn</b>	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.

# hostname

To set the security appliance 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

<i>name</i>	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 hostname depends on your platform.

## Command Modes

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

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

## Command History

Release	Modification
7.0(1)	You can no longer use non-alphanumeric characters (other than a hyphen).

## 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
firewall1(config)#
```

## Related Commands

Command	Description
<b>banner</b>	Sets a login, message of the day, or enable banner.
<b>domain-name</b>	Sets the default domain name.

## html-content-filter

To filter Java, ActiveX, images, scripts, and cookies for WebVPN sessions for this user or group policy, use the **html-content-filter** command in webvpn mode, which you enter from group-policy or username mode. To remove a content filter, use the **no** form of this command. To remove all content filters, including a null value created by issuing the **html-content-filter none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting an html content filter, use the **html-content-filter none** command.

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

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

### Syntax Description

<b>cookies</b>	Removes cookies from images, providing limited ad filtering and privacy.
<b>images</b>	Removes references to images (removes <IMG> tags).
<b>java</b>	Removes references to Java and ActiveX (removes <EMBED>, <APPLET>, and <OBJECT> tags).
<b>none</b>	Indicates that there is no filtering. Sets a null value, thereby disallowing filtering. Prevents inheriting filtering values.
<b>scripts</b>	Removes references to scripting (removes <SCRIPT> tags).

### Defaults

No filtering occurs.

### Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn mode	•	—	•	—	—

### Command History

Release	Modification
7.0(1)	This command was introduced.

### Usage Guidelines

Using the command a second time overrides the previous setting.

### Examples

The following example shows how to set filtering of JAVA and ActiveX, cookies, and images for the group policy named FirstGroup:

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

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>webvpn (group-policy, username)</b>	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
<b>webvpn</b>	Use in global configuration mode. Lets you configure global settings for WebVPN.

# http

To specify hosts that can access the HTTP server internal to the security appliance, 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

<i>interface_name</i>	Provides the name of the security appliance interface through which the host can access the HTTP server.
<i>ip_address</i>	Provides the IP address of a host that can access the HTTP server.
<i>subnet_mask</i>	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:

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

## Command History

Release	Modification
Preexisting	This command was preexisting.

## 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
<b>clear configure http</b>	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
<b>http authentication-certificate</b>	Requires authentication via certificate from users who are establishing HTTPS connections to the security appliance.

<b>Command</b>	<b>Description</b>
<b>http redirect</b>	Specifies that the security appliance redirect HTTP connections to HTTPS.
<b>http server enable</b>	Enables the HTTP server.
<b>show running-config http</b>	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** version of this command. To remove all **http authentication-certificate** commands from the configuration, use the **no** version without arguments.

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

**http authentication-certificate** *interface*

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

## Syntax Description

*interface* Specifies the interface on the security appliance 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:

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Usage Guidelines

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
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>clear configure http</b>	Removes the HTTP configuration: disables the HTTP server and removes hosts that can access the HTTP server.
	<b>http</b>	Specifies hosts that can access the HTTP server by IP address and subnet mask. Specifies the security appliance interface through which the host accesses the HTTP server.
	<b>http redirect</b>	Specifies that the security appliance redirect HTTP connections to HTTPS.
	<b>http server enable</b>	Enables the HTTP server.
	<b>show running-config http</b>	Displays the hosts that can access the HTTP server, and whether or not the HTTP server is enabled.

# http-comp

To enable compression of http data over a WebVPN connection for a specific group or user, use the **http-comp** command in the group policy and username webvpn modes.

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command:

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

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

## Syntax Description

<b>gzip</b>	Specifies compression is enabled for the group or user.
<b>none</b>	Specifies compression is disabled for the group or user.

## Defaults

By default, compression is set to *gzip*.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
group-policy webvpn	•	—	•	—	—
username webvpn	•	—	•	—	—

## Command History

Release	Modification
7.1.1	This command was introduced.

## Usage Guidelines

For WebVPN connections, the **compression** command configured from global configuration mode overrides the **http-comp** command configured in group policy and username webvpn modes.

## Examples

In the following example, compression is disabled for the group-policy sales:

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

## Related Commands

Command	Description
<b>compression</b>	Enables compression for all SVC, WebVPN, IPsec VPN connections.

# 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:

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

## Command History

Release	Modification
7.0(1)	This command was introduced in 7.0(1).

## 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 security appliance 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. Click on an entry to open a command page that provides the detailed syntax for each command.

**Table 13-2 HTTP Map Configuration Commands**

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

**Examples**

The following is sample output showing 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 security appliance 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**

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

# http-proxy

To configure an HTTP proxy server, use the **http-proxy** command in webvpn mode. To remove the HTTP proxy server from the configuration, use the **no** form of this command.

This is an external proxy server the security appliance uses for HTTP requests.

**http-proxy** *address* [*port*]

**no http-proxy**

## Syntax Description

<i>address</i>	Specifies the IP address for the external HTTP proxy server.
<i>port</i>	Specifies the port the HTTP proxy server uses. The default port is 80, which is the port the security appliance uses if you do not supply a value.

## Defaults

No HTTP proxy server is configured by default.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn	•	—	•	—	—

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Examples

The following example shows how to configure an HTTP proxy server with an IP address of 10.10.10.7 using port 80:

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

# http redirect

To specify that the security appliance redirect HTTP connections to HTTPS, use the **http redirect** command in global configuration mode. To remove a specified http redirect command from the configuration, use the **no** version of this command. To remove all http redirect commands from the configuration, use the **no** version of this command without arguments.

**http redirect** *interface* [*port*]

**no http redirect** [*interface*]

## Syntax Description

<i>interface</i>	Identifies the interface for which the security appliance should redirect HTTP requests to HTTPS.
<i>port</i>	Identifies the port the security appliance listens on for HTTP requests, which it then redirects to HTTPS. By default it listens on port 80,

## Defaults

HTTP redirect is disabled.

## Command Modes

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

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

## Command History

Release	Modification
7.0(1)	This command was introduced.

## Usage Guidelines

The interface requires an access list that permits HTTP. Otherwise the security appliance does not listen to port 80, or to any other port that you configure for HTTP.

## Examples

The following example shows how to configure HTTP redirect for the inside interface, keeping the default port 80:

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

## Related Commands

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

# http server enable

To enable the security appliance HTTP server, use the **http server enable** command in global configuration mode. To disable the HTTP 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:

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

## Command History

Release	Modification
Preexisting	This command was preexisting.

## Examples

The following example shows how to enable the HTTP server.

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

## Related Commands

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

# https-proxy

To configure an HTTPS proxy server, use the **https-proxy** command in webvpn mode. To remove the HTTPS proxy server from the configuration, use the no form of this command.

This is an external proxy server the security appliance uses for HTTPS requests.

```
https-proxy address [port]
```

```
no https-proxy
```

## Syntax Description

<i>address</i>	Specifies the IP address for the external HTTPS proxy server.
<i>port</i>	Specifies the port the HTTPS proxy server uses. The default port is 443, which is the port the security appliance uses if you do not supply a value.

## Defaults

No HTTPS proxy server is configured by default.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Webvpn	•	—	•	—	—

## Command History

Release	Modification
7.0.1	This command was introduced.

## Examples

The following example shows how to configure an HTTPS proxy server with an IP address of 10.10.10.1 using port 443:

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

# hw-module module recover

To load a recovery software image from a TFTP server to an intelligent SSM (for example, the AIP SSM), or to configure network settings to access the TFTP server, use the **hw-module module recover** command in privileged EXEC mode. You might need to recover an SSM using this command if, for example, the SSM is unable to load a local image. This command is not available for interface SSMs (for example, the 4GE SSM).

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

## Syntax Description

<b>1</b>	Specifies the slot number, which is always 1.
<b>boot</b>	Initiates recovery of this SSM and downloads a recovery image according to the <b>configure</b> settings. The SSM then reboots from the new image.
<b>configure</b>	Configures the network parameters to download a recovery image. If you do not enter any network parameters after the <b>configure</b> keyword, you are prompted for the information.
<b>gateway</b> <i>gateway_ip_address</i>	(Optional) The gateway IP address for access to the TFTP server through the SSM management interface.
<b>ip</b> <i>port_ip_address</i>	(Optional) The IP address of the SSM management interface.
<b>stop</b>	Stops the recovery action, and stops downloading the recovery image. The SSM boots from the original image. You must enter this command within 30 to 45 seconds after starting recovery using the <b>hw-module module boot</b> command. If you issue the <b>stop</b> command after this period, it might cause unexpected results, such as the SSM becoming unresponsive.
<b>url</b> <i>tftp_url</i>	(Optional) The URL for the image on a TFTP server, in the following format: <b>tftp://server/[path/]filename</b>
<b>vlan</b> <i>vlan_id</i>	(Optional) Sets the VLAN ID for the management interface.

## Defaults

No default behavior or values.

## Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

## Command History

Release	Modification
7.0(1)	This command was introduced.

**Usage Guidelines**

This command is only available when the SSM is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information.

**Examples**

The following example sets the SSM to download an image from a TFTP server:

```
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
```

The following example recovers the SSM:

```
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]
```

**Related Commands**

Command	Description
<b>debug module-boot</b>	Shows debug messages about the SSM booting process.
<b>hw-module module reset</b>	Shuts down an SSM and performs a hardware reset.
<b>hw-module module reload</b>	Reloads the intelligent SSM software.
<b>hw-module module shutdown</b>	Shuts down the SSM software in preparation for being powered off without losing configuration data.
<b>show module</b>	Shows SSM information.

# hw-module module reload

To reload an intelligent SSM software (for example, the AIP SSM), use the **hw-module module reload** command in privileged EXEC mode. This command is not available for interface SSMs (for example, the 4GE SSM).

## hw-module module 1 reload

<b>Syntax Description</b>	<b>1</b> Specifies the slot number, which is always 1.
---------------------------	--

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	The following table shows the modes in which you can enter the command:
----------------------	---

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

<b>Command History</b>	<b>Release</b>	<b>Modification</b>
	7.0(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>This command is only valid when the SSM status is Up. See the <b>show module</b> command for state information.</p> <p>This command differs from the <b>hw-module module reset</b> command, which also performs a hardware reset.</p>
-------------------------	--

<b>Examples</b>	The following example reloads the SSM in slot 1:
-----------------	--

```
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.
```

<b>Related Commands</b>	<b>Command</b>	<b>Description</b>
	<b>debug module-boot</b>	Shows debug messages about the SSM booting process.
	<b>hw-module module recover</b>	Recovers an intelligent SSM by loading a recovery image from a TFTP server.

<b>Command</b>	<b>Description</b>
<b>hw-module module reset</b>	Shuts down an SSM and performs a hardware reset.
<b>hw-module module shutdown</b>	Shuts down the SSM software in preparation for being powered off without losing configuration data.
<b>show module</b>	Shows SSM information.

# hw-module module reset

To shut down and reset the SSM hardware, use the **hw-module module reset** command in privileged EXEC mode.

## hw-module module 1 reset

### Syntax Description

**1** Specifies the slot number, which is always 1.

### Defaults

No default behavior or values.

### Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

### Command History

Release	Modification
7.0(1)	This command was introduced.

### Usage Guidelines

This command is only valid when the SSM status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

When the SSM is in an Up state, the **hw-module module reset** command prompts you to shut down the software before resetting.

You can recover intelligent SSMs (for example, the AIP SSM) using the **hw-module module recover** command. If you enter the **hw-module module reset** while the SSM is in a Recover state, the SSM does not interrupt the recovery process. The **hw-module module reset** command performs a hardware reset of the SSM, and the SSM recovery continues after the hardware reset. You might want to reset the SSM during recovery if the SSM hangs; a hardware reset might resolve the issue.

This command differs from the **hw-module module reload** command which only reloads the software and does not perform a hardware reset.

### Examples

The following example resets an SSM in slot 1 that is in the Up state:

```
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.
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>debug module-boot</b>	Shows debug messages about the SSM booting process.
<b>hw-module module recover</b>	Recovers an intelligent SSM by loading a recovery image from a TFTP server.
<b>hw-module module reload</b>	Reloads the intelligent SSM software.
<b>hw-module module shutdown</b>	Shuts down the SSM software in preparation for being powered off without losing configuration data.
<b>show module</b>	Shows SSM information.

# hw-module module shutdown

To shut down the SSM software, use the **hw-module module shutdown** command in privileged EXEC mode.

## hw-module module 1 shutdown

<b>Syntax Description</b>	<b>1</b>	Specifies the slot number, which is always 1.
---------------------------	----------	---

<b>Defaults</b>	No default behavior or values.
-----------------	--------------------------------

<b>Command Modes</b>	The following table shows the modes in which you can enter the command:
----------------------	---

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Privileged EXEC	•	•	•	—	•

Command History	Release	Modification
	7.0(1)	This command was introduced.

<b>Usage Guidelines</b>	<p>Shutting down the SSM software prepares the SSM to be safely powered off without losing configuration data.</p> <p>This command is only valid when the SSM status is Up or Unresponsive. See the <b>show module</b> command for state information.</p>
-------------------------	---

<b>Examples</b>	<p>The following example shuts down an SSM in slot 1:</p> <pre>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.</pre>
-----------------	---

Related Commands	Command	Description
	<b>debug module-boot</b>	Shows debug messages about the SSM booting process.
	<b>hw-module module recover</b>	Recovers an intelligent SSM by loading a recovery image from a TFTP server.

<b>Command</b>	<b>Description</b>
<b>hw-module module reload</b>	Reloads the intelligent SSM software.
<b>hw-module module reset</b>	Shuts down an SSM and performs a hardware reset.
<b>show module</b>	Shows SSM information.

