



## quit through router-id Commands

---

# quit

To exit the current configuration mode, or to log out from privileged or user EXEC modes, use the **quit** command.

## quit

**Syntax Description** This command has no arguments or keywords.

**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
User EXEC	•	•	•	•	•

Command History	Release	Modification
	1.1(1)	This command was introduced.

**Usage Guidelines** You can also use the key sequence **Ctrl Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **quit** command in privileged or user EXEC modes, you log out from the FWSM. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

**Examples** The following example shows how to use the **quit** command to exit global configuration mode, and then logout from the session:

```
hostname(config)# quit
hostname# quit
```

Logoff

The following example shows how to use the **quit** command to exit global configuration mode, and then use the **disable** command to exit privileged EXEC mode:

```
hostname(config)# quit
hostname# disable
hostname>
```

## Related Commands

Command	Description
exit	Exits a configuration mode or logs out from privileged or user EXEC modes.

# radius-common-pw

To specify a common password to be used for all users whose VPN access is authorized by a RADIUS authorization server, use the **radius-common-pw** command in AAA-server host mode. To remove this specification, use the **no** form of this command:

```
radius-common-pw password
```

```
no radius-common-pw
```

## Syntax Description

<i>password</i>	A case-sensitive, alphanumeric keyword of up to 127 characters to be used as a common password for all authorization transactions with the RADIUS server specified with the <b>aaa-server host</b> command.
-----------------	---

## 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
Aaa-server host	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

This command is valid only for RADIUS authorization servers.

The RADIUS authorization server requires a password and username for each connecting user. The FWSM provides the username automatically. You enter the password here. The RADIUS server administrator must configure the RADIUS server to associate this password with each user authorizing to the server via this FWSM. Be sure to provide this information to your RADIUS server administrator.

If you do not specify a common user password, each user password is the username of the user. For example, the default RADIUS authorization for a user with the username “jsmith” is “jsmith”. If you are using usernames for the common user passwords, as a security precaution do not use this RADIUS server for authorization anywhere else on your network.



### Note

The password field is required by the RADIUS protocol and the RADIUS server requires it; however, users do not need to know it.

**Examples**

The following example configures a RADIUS AAA server group named “svrgrp1” on host “1.2.3.4”, sets the timeout interval to 9 seconds, sets the retry interval to 7 seconds, and configures the RADIUS common password as “allauthpw”.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>aaa-server host</b>	Enter AAA server host configuration mode so that you can configure AAA server parameters that are host-specific.
<b>clear configure aaa-server</b>	Remove all AAA command statements from the configuration.
<b>show running-config aaa-server</b>	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

# radius-with-expiry

To have the FWSM use MS-CHAPv2 to negotiate a password update with the user during authentication, use the **radius-with-expiry** command in tunnel-group ipsec-attributes configuration mode. The FWSM ignores this command if RADIUS authentication has not been configured.

To return to the default value, use the **no** form of this command.

**radius-with-expiry**

**no radius-with-expiry**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default setting for this command 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
Tunnel-group ipsec-attributes configuration	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

You can apply this attribute to IPsec remote-access tunnel-group type only.

## Examples

The following example entered in config-ipsec configuration mode, configures Radius with Expiry for the remote-access tunnel group named remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# radius-with-expiry
hostname(config-ipsec)#
```

## Related Commands

Command	Description
<b>clear configure tunnel-group</b>	Clears all configured tunnel groups.
<b>show running-config tunnel-group</b>	Shows the indicated certificate map entry.
<b>tunnel-group-map default-group</b>	Associates the certificate map entries created using the <b>crypto ca certificate map</b> command with tunnel groups.

# reactivation-mode

To specify the method (reactivation policy) by which failed servers in a group are reactivated, use the **reactivation-mode** command in AAA-server group mode. To remove this specification, use the **no** form of this command:

**reactivation-mode depletion** [*deadtime minutes*]

**reactivation-mode timed**

**no reactivation-mode**

## Syntax Description

<b>deadtime</b> <i>minutes</i>	(Optional) Specifies the amount of time that elapses between the disabling of the last server in the group and the subsequent reenabling of all servers.
<b>depletion</b>	Reactivates failed servers only after all of the servers in the group are inactive.
<b>timed</b>	Reactivates failed servers after 30 seconds of down time.

## Defaults

The default reactivation mode is depletion, and the default deadtime value is 10. The supported range of values for deadtime is 0-1440 minutes.

## 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 group	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

Each server group has an attribute that specifies the reactivation policy for its servers.

In **depletion** mode, when a server is deactivated, it remains inactive until all other servers in the group are inactive. When and if this occurs, all servers in the group are reactivated. This approach minimizes the occurrence of connection delays due to failed servers. When **depletion** mode is in use, you can also specify the **deadtime** parameter. The **deadtime** parameter specifies the amount of time (in minutes) that will elapse between the disabling of the last server in the group and the subsequent re-enabling of all servers. This parameter is meaningful only when the server group is being used in conjunction with the local fallback feature.

In **timed** mode, failed servers are reactivated after 30 seconds of down time. This is useful when customers use the first server in a server list as the primary server and prefer that it is online whenever possible. This policy breaks down in the case of UDP servers. Because UDP is a connectionless protocol,

the FWSM cannot determine if the server is present; therefore, UDP servers are put back on line blindly. This could lead to slowed connection times or connection failures if a server list contains multiple servers that are not reachable.

Accounting server groups that have simultaneous accounting enabled are forced to use the **timed** mode. This implies that all servers in a given list are equivalent.

### Examples

The following example configures a TACACS+ AAA server named “svrgrp1” to use the depletion reactivation mode, with a deadtime of 15 minutes:

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-servers-group)# reactivation-mode depletion deadtime 15
```

The following example configures a TACACS+ AAA server named “svrgrp1” to use timed reactivation mode:

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
```

### Related Commands

<b>accounting-mode</b>	Indicates whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
<b>aaa-server protocol</b>	Enters AAA server group configuration mode so that you can configure AAA server parameters that are group-specific and common to all hosts in the group.
<b>max-failed-attempts</b>	Specifies the number of failures that will be tolerated for any given server in the server group before that server is deactivated.
<b>clear configure aaa-server</b>	Removes all AAA server configuration.
<b>show running-config aaa-server</b>	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol

# redistribute

To redistribute routes from one routing domain into another routing domain, use the **redistribute** command in router configuration mode. To remove the redistribution, use the **no** form of this command.

```
redistribute {{ ospf pid [match { internal | external [ 1 | 2 ] | nssa-external [ 1 | 2 ] }} | static |
connected } [metric metric_value] [metric-type metric_type] [route-map map_name] [tag
tag_value] [subnets]
```

```
no redistribute {{ ospf pid [match { internal | external [ 1 | 2 ] | nssa-external [ 1 | 2 ] }} | static |
connected } [metric metric_value] [metric-type metric_type] [route-map map_name] [tag
tag_value] [subnets]
```

Syntax Description		
<b>connected</b>		Specifies redistributing a network connected to an interface into an OSPF routing process.
<b>external</b> <i>type</i>		Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are <b>1</b> or <b>2</b> .
<b>internal</b> <i>type</i>		Specifies OSPF metric routes that are internal to a specified autonomous system.
<b>match</b>		(Optional) Specifies the conditions for redistributing routes from one routing protocol into another.
<b>metric</b> <i>metric_value</i>		(Optional) Specifies the OSPF default metric value from 0 to 16777214.
<b>metric-type</b> <i>metric_type</i>		(Optional) The external link type associated with the default route advertised into the OSPF routing domain. It can be either of the following two values: 1 (Type 1 external route) or 2 (Type 2 external route).
<b>nssa-external</b> <i>type</i>		Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are <b>1</b> or <b>2</b> .
<b>ospf</b> <i>pid</i>		Used to redistribute an OSPF routing process into the current OSPF routing process. The <i>pid</i> specifies the internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
<b>route-map</b> <i>map_name</i>		(Optional) Name of the route map to apply.
<b>static</b>		Used to redistribute a static route into an OSPF process.
<b>subnets</b>		(Optional) For redistributing routes into OSPF, scopes the redistribution for the specified protocol. If not used, only classful routes are redistributed.
<b>tag</b> <i>tag_value</i>		(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

## 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
Router configuration	•	—	•	—	—

**Command History**

Release	Modification
1.1(1)	This command was introduced.

**Examples**

This example shows how to redistribute static routes into the current OSPF process:

```
hostname(config-router)# redistribute ospf static
```

**Related Commands**


Command	Description
<b>router ospf</b>	Enters router configuration mode.
<b>show running-config router</b>	Displays the commands in the global router configuration.

# reload

To reboot and reload the configuration, use the **reload** command in privileged EXEC mode.

```
reload [at hh:mm [month day | day month]] [cancel] [in [hh:mm]] [max-hold-time [hh:mm]]
[noconfirm] [quick] [reason text] [save-config]
```

## Syntax Description

<b>at</b> <i>hh:mm</i>	(Optional) Schedules a reload of the software to take place at the specified time (using a 24-hour clock). If you do not specify the month and day, the reload occurs at the specified time on the current day (if the specified time is later than the current time), or on the next day (if the specified time is earlier than the current time). Specifying 00:00 schedules the reload for midnight. The reload must take place within 24 hours.
<b>cancel</b>	(Optional) Cancels a scheduled reload.
<i>day</i>	(Optional) Number of the day in the range from 1 to 31.
<b>in</b> [ <i>hh:mm</i> ]	(Optional) Schedules a reload of the software to take effect in the specified minutes or hours and minutes. The reload must occur within 24 hours.
<b>max-hold-time</b> [ <i>hh:mm</i> ]	(Optional) Specifies the maximum hold time the FWSM waits to notify other subsystems before a shutdown or reboot. After this time elapses, a quick (forced) shutdown/reboot occurs.
<i>month</i>	(Optional) Specifies the name of the month. Enter enough characters to create a unique string for the name of the month. For example, “Ju” is not unique because it could represent June or July, but “Jul” is unique because no other month beginning with those exact three letters.
<b>noconfirm</b>	(Optional) Permits the FWSM to reload without user confirmation.
<b>quick</b>	(Optional) Forces a quick reload, without notifying or properly shutting down all the subsystems.
<b>reason</b> <i>text</i>	(Optional) Specifies the reason for the reload, 1 to 255 characters. The reason text is sent to all open IPsec VPN client, terminal, console, telnet, SSH, and ASDM connections/sessions.
	 <p><b>Note</b> Some applications, like isakmp, require additional configuration to send the reason text to IPsec VPN Clients. Refer to the appropriate section in the software configuration documentation for more information.</p>
<b>save-config</b>	(Optional) Saves the running configuration to memory before shutting down. If you do not enter the <b>save-config</b> keyword, any configuration changes that have not been saved will be lost after the reload.

## 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
3.1(1)	This command was modified to add the following new arguments and keywords: <i>day</i> , <i>hh</i> , <i>mm</i> , <i>month</i> , <b>quick</b> , <b>save-config</b> , and <i>text</i> .

**Usage Guidelines**

The `reload` command lets you reboot the FWSM and reload the configuration from Flash.

By default, the **reload** command is interactive. The FWSM first checks whether the configuration has been modified but not saved. If so, the FWSM prompts you to save the configuration. In multiple context mode, the FWSM prompts for each context with an unsaved configuration. If you specify the **save-config** parameter, the configuration is saved without prompting you. The FWSM then prompts you to confirm that you really want to reload the system. Only a response of **y** or pressing the **Enter** key causes a reload. Upon confirmation, the FWSM starts or schedules the reload process, depending upon whether you have specified a delay parameter (**in** or **at**).

By default, the reload process operates in “graceful” (also known as “nice”) mode. All registered subsystems are notified when a reboot is about to occur, allowing these subsystems to shut down properly before the reboot. To avoid waiting until for such a shutdown to occur, specify the **max-hold-time** parameter to specify a maximum time to wait. Alternatively, you can use the **quick** parameter to force the reload process to begin abruptly, without notifying the affected subsystems or waiting for a graceful shutdown.

You can force the **reload** command to operate noninteractively by specifying the **noconfirm** parameter. In this case, the FWSM does not check for an unsaved configuration unless you have specified the **save-config** parameter. The FWSM does not prompt the user for confirmation before rebooting the system. It starts or schedules the reload process immediately, unless you have specified a delay parameter, although you can specify the **max-hold-time** or **quick** parameters to control the behavior or the reload process.

Use **reload cancel** to cancel a scheduled reload. You cannot cancel a reload that is already in progress.

**Note**

Configuration changes that are not written to the Flash partition are lost after a reload. Before rebooting, enter the **write memory** command to store the current configuration in the Flash partition.

**Examples**

This example shows how to reboot and reload the configuration:

```
hostname# reload
Proceed with ? [confirm] y

Rebooting...

XXX Bios VX.X
...
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>show reload</b>	Displays the reload status of the FWSM.

# remote-access threshold session-threshold-exceeded

To set threshold values, use the **remote-access threshold session-threshold-exceeded** command in global configuration mode. To remove threshold values, use the **no** version of this command. This command specifies the number of remote access sessions that need to be active for the FWSM to send traps.

**remote-access threshold session-threshold-exceeded** {*threshold-value*}

**no remote-access threshold session-threshold-exceeded**

<b>Syntax Description</b>	<i>threshold-value</i>	Specifies an integer less than or equal to the session limit the FWSM supports.
---------------------------	------------------------	---

**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
	3.1(1)	This command was introduced.

**Examples** The following example shows how to set a threshold value of 1500:

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

Related Commands	Command	Description
	<b>snmp-server enable trap</b>	Enables threshold trapping.
	<b>remote-access</b>	

# rename

To rename a file or a directory from the source filename to the destination filename, use the **rename** command in privileged EXEC mode.

**rename** [/noconfirm] [flash:] *source-path* [flash:] *destination-path*

## Syntax Description

<b>/noconfirm</b>	(Optional) Suppresses the confirmation prompt.
<b><i>destination-path</i></b>	Specifies the path of the destination file.
<b>flash:</b>	(Optional) Specifies the internal flash memory, followed by a colon.
<b><i>source-path</i></b>	Specifies the path of the source file.

## 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
3.1(1)	Support for this command was introduced.

## Usage Guidelines

The **rename flash: flash:** command prompts you to enter a source and destination filename.

You cannot rename a file or directory across file systems.

For example:

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

## Examples

The following example shows how to rename a file named “test” to “test1”:

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

## Related Commands

<b>Command</b>	<b>Description</b>
<b>mkdir</b>	Creates a new directory.
<b>rmdir</b>	Removes a directory.
<b>show file</b>	Displays information about the file system.

# replication http

To enable HTTP connection replication for the failover group, use the **replication http** command in failover group configuration mode. To disable HTTP connection replication, use the **no** form of this command.

**replication http**

**no replication http**

## Syntax Description

This command has no arguments or keywords.

## Defaults

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
Failover group configuration	•	•	—	—	•

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

By default, the FWSM does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative effect on system performance.

This command is available for Active/Active failover only. It provides the same functionality as the **failover replication http** command for Active/Standby failover, except for failover groups in Active/Active failover configurations.

## Examples

The following example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

Related Commands	Command	Description
	<b>failover group</b>	Defines a failover group for Active/Active failover.
	<b>failover replication http</b>	Configures Stateful Failover to replicate HTTP connections.

# request-command deny

To disallow specific commands within FTP requests, use the **request-command deny** command in FTP map configuration mode, which is accessible by using the **ftp-map** command. To remove the configuration, use the **no** form of this command.

```
request-command deny { appe | cdup | dele | get | help | mkd | put | rmd | rnfr | rnto | site | stou }
```

```
no request-command deny { appe | cdup | help | retr | rnfr | rnto | site | stor | stou }
```

## Syntax Description

<b>appe</b>	Disallows the command that appends to a file.
<b>cdup</b>	Disallows the command that changes to the parent directory of the current working directory.
<b>dele</b>	Disallows the command that deletes a file on the server.
<b>get</b>	Disallows the client command for retrieving a file from the server.
<b>help</b>	Disallows the command that provides help information.
<b>mkd</b>	Disallows the command that makes a directory on the server.
<b>put</b>	Disallows the client command for sending a file to the server.
<b>rmd</b>	Disallows the command that deletes a directory on the server.
<b>rnfr</b>	Disallows the command that specifies rename-from filename.
<b>rnto</b>	Disallows the command that specifies rename-to filename.
<b>site</b>	Disallows the command that are specific to the server system. Usually used for remote administration.
<b>stou</b>	Disallows the command that stores a file using a unique filename.

## 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
FTP map configuration	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

This command is used for controlling the commands allowed within FTP requests traversing the FWSM when using strict FTP inspection.

**Examples**

The following example causes the FWSM to drop FTP requests containing **stor**, **stou**, or **appe** commands:

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
```

**Related Commands**

Commands	Description
<b>class-map</b>	Defines the traffic class to which to apply security actions.
<b>ftp-map</b>	Defines an FTP map and enables FTP map configuration mode.
<b>inspect ftp</b>	Applies a specific FTP map to use for application inspection.
<b>mask-syst-reply</b>	Hides the FTP server response from clients.
<b>policy-map</b>	Associates a class map with specific security actions.

# request-method

To restrict HTTP traffic based on the HTTP request method, use the **request-method** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

```
request-method { { ext ext_methods | default } | { rfc rfc_methods | default } } action { allow | reset | drop } [log]
```

```
no request-method { ext ext_methods | rfc rfc_methods } action { allow | reset | drop } [log]
```

## Syntax Description

<b>action</b>	Identifies the action taken when a message fails this command inspection.
<b>allow</b>	Allows the message.
<b>default</b>	Specifies the default action taken by the FWSM when the traffic contains a supported request method that is not on a configured list.
<b>drop</b>	Closes the connection.
<b>ext</b>	Specifies extension methods.
<i>ext-methods</i>	Identifies one of the extended methods you want to allow to pass through the FWSM.
<b>log</b>	(Optional) Generates a syslog.
<b>reset</b>	Sends a TCP reset message to client and server.
<b>rfc</b>	Specifies RFC 2616 supported methods.
<i>rfc-methods</i>	Identifies one of the RFC methods you want to allow to pass through the FWSM (see <a href="#">Table 23-1</a> ).

## Defaults

This command is disabled by default. When the command is enabled and a supported request method is not specified, the default action is to allow the connection without logging. To change the default action, use the **default** keyword and specify a different default action.

## 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
HTTP map configuration	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

**Usage Guidelines**

When you enable the **request-method** command, the FWSM applies the specified action to HTTP connections for each supported and configured request method.

The FWSM applies the **default** action to all traffic that does *not* match the request methods on the configured list. The **default** action is to **allow** connections without logging. Given this preconfigured default action, if you specify one or more request methods with the action of **drop** and **log**, the FWSM drops connections containing the configured request methods, logs each connection, and allows all connections containing other supported request methods.

If you want to configure a more restrictive policy, change the default action to **drop** (or **reset**) and **log** (if you want to log the event). Then configure each permitted method with the **allow** action.

Enter the **request-method** command once for each setting you wish to apply. You use one instance of the **request-method** command to change the default action or to add a single request method to the list of configured methods.

When you use the **no** form of the command to remove a request method from the list of configured methods, any characters in the command line after the request method keyword are ignored.

Table 23-1 lists the methods defined in RFC 2616 that you can add to the list of configured methods:

**Table 23-1 RFC 2616 Methods**

Method	Description
connect	Used with a proxy that can dynamically switch to being a tunnel (for example SSL tunneling).
delete	Requests that the origin server delete the resource identified by the Request-URI.
get	Retrieves whatever information or object is identified by the Request-URI.
head	Identical to GET except that the server does not return a message-body in the response.
options	Represents a request for information about the communication options available on server identified by the Request-URI.
post	Request that the origin server accept the object enclosed in the request as a new subordinate of the resource identified by the Request-URI in the Request-Line.
put	Requests that the enclosed object be stored under the supplied Request-URI.
trace	Invokes a remote, application-layer loop-back of the request message.

**Examples**

The following example provides a permissive policy, using the preconfigured default, which allows all supported request methods that are not specifically prohibited.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc options drop log
hostname(config-http-map)# request-method rfc post drop log
```

In this example, only the **options** and **post** request methods are dropped and the events are logged.

The following example provides a restrictive policy, with the default action changed to **reset** the connection and **log** the event for any request method that is not specifically allowed.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc default action reset log
hostname(config-http-map)# request-method rfc get allow
hostname(config-http-map)# request-method rfc put allow
```

In this case, the **get** and **put** request methods are allowed. When traffic is detected that uses any other methods, the FWSM resets the connection and creates a syslog entry.

<b>Related Commands</b>	<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 traffic associated with enhanced HTTP inspection.
	<b>http-map</b>	Defines an HTTP map for configuring enhanced HTTP inspection.
	<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.

# request-queue

To specify the maximum number of GTP requests that will be queued waiting for a response, use the **request-queue** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. To return this number to the default of 200, use the **no** form of this command.

```
request-queue max_requests
```

```
no request-queue max_requests
```

## Syntax Description

<i>max_requests</i>	The maximum number of GTP requests that will be queued waiting for a response. The range values is 1 to 4294967295.
---------------------	---

## Defaults

The *max\_requests* default is 200.

## 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
GTP map configuration	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

The **gtp request-queue** command specifies the maximum number of GTP requests that are queued waiting for a response. When the limit has been reached and a new request arrives, the request that has been in the queue for the longest time is removed. The Error Indication, the Version Not Supported and the SGSN Context Acknowledge messages are not considered as requests and do not enter the request queue to wait for a response.

## Examples

The following example specifies a maximum request queue size of 300 bytes:

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# request-queue-size 300
```

## Related Commands

Commands	Description
<b>clear service-policy</b> <b>inspect gtp</b>	Clears global GTP statistics.
<b>debug gtp</b>	Displays detailed information about GTP inspection.

<b>Commands</b>	<b>Description</b>
<b>gtp-map</b>	Defines a GTP map and enables GTP map configuration mode.
<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.

# resource acl-partition

To reduce the number of memory partitions in multiple context mode from the maximum of 12, use the **resource acl-partition** command in global configuration mode. To restore the number of partitions to 12, use the **no** form of this command. In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. You might want to reduce the number of partitions to better match the number of contexts you have.

**resource acl-partition** *number*

**no resource acl-partition** *number*

## Syntax Description

*number* Specifies the number of partitions, between 1 and 12.

**Note** If you assign a context to a partition, the partition numbering starts with 0. So if you have 12 partitions, the partition numbers are 0 through 11.

## Defaults

The FWSM uses 12 memory partitions 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	N/A	N/A	—	—	•

## Command History

Release	Modification
2.3(1)	This command was introduced.

## Usage Guidelines

In multiple context mode, the FWSM partitions the memory allocated to rule configuration, and assigns each context to a partition. By default, a context belongs to one of 12 partitions that offers a maximum of 12,130 rules, including ACEs, AAA rules, and others. The FWSM assigns contexts to the partitions in the order they are loaded at startup. For example, if you have 12 contexts, each context is assigned to its own partition, and can use 12,130 rules. If you add one more context, then context number 1 and the new context number 13 are both assigned to partition 1, and can use 12,130 rules divided between them; the other 11 contexts continue to use 12,130 rules each. If you delete contexts, the partition membership does not shift, so you might have some unequal distribution until you reboot, at which time the contexts are evenly distributed.



### Note

Rules are used up on a first come, first served basis, so one context might use more rules than another context.

You can manually assign a context to a partition with the **allocate-acl-partition** command.

Changing the number of partitions requires you to reload the FWSM. If you are using failover, you must also reload the other failover unit because the memory partitions must match on both units. Traffic loss can occur because both units are down at the same time.

**Note**

If you later enter the **clear configure all** command to restore the default configuration, the **resource acl-partition** command is not changed back to the default. You must enter the **no resource acl-partition** command to restore the default for this command.

**Examples**

The following example partitions the memory into 8 parts:

```
hostname(config)# resource acl-partition 8
```

This configuration command leads to repartitioning of ACL memory. It will not take effect unless you save the configuration to startup configuration and reboot. Would you like to save the configuration and reboot now? [n]

**Related Commands**

Command	Description
<b>allocate-acl-partition</b>	Assigns a context to a specific memory partition.
<b>context</b>	Configures a security context.
<b>show resource acl-partition</b>	Shows the contexts assigned to each memory partition and the number of rules used.

# retry-interval

To configure the amount of time between retry attempts for a particular AAA server designated in a prior **aaa-server host** command, use the **retry-interval** command in AAA-server host mode. To reset the retry interval to the default value, use the **no** form of this command.

**retry-interval** *seconds*

**no retry-interval**

## Syntax Description

*seconds* Specify the retry interval (1-10 seconds) for the request. This is the time the FWSM waits before retrying a connection request.

## Defaults

The default retry interval is 10 seconds.

## 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	•	•	•	•	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

Use the **retry-interval** command to specify or reset the number of seconds the FWSM waits between connection attempts. Use the **timeout** command to specify the length of time during which the FWSM attempts to make a connection to a AAA server.

## Examples

The following examples show the **retry-interval** command in context.

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
```

## Related Commands

Command	Description
<b>aaa-server host</b>	Enters AAA server host configuration mode so that you can configure AAA server parameters that are host-specific.

<b>clear configure aaa-server</b>	Removes all AAA command statements from the configuration.
<b>show running-config aaa-server</b>	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.
<b>timeout</b>	Specifies the length of time during which the FWSM attempts to make a connection to a AAA server.

# re-xauth

To require that users reauthenticate on IKE rekey, issue the **re-xauth enable** command in group-policy configuration mode. To disable user reauthentication on IKE rekey, use the **re-xauth disable** command.

To remove the re-xauth attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for reauthentication on IKE rekey from another group policy.

**re-xauth {enable | disable}**

**no re-xauth**

## Syntax Description

<b>disable</b>	Disables reauthentication on IKE rekey
<b>enable</b>	Enables reauthentication on IKE rekey

## Defaults

Reauthentication on IKE rekey 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
Group policy	•	—	•	—	—

## Command History

Release	Modification
3.1(1)	This command was introduced.

## Usage Guidelines

If you enable reauthentication on IKE rekey, the FWSM prompts the user to enter a username and password during initial Phase 1 IKE negotiation and also prompts for user authentication whenever an IKE rekey occurs. Reauthentication provides additional security.

If the configured rekey interval is very short, users might find the repeated authorization requests inconvenient. In this case, disable reauthentication. To check the configured rekey interval, in monitoring mode, issue the **show crypto ipsec sa** command to view the security association lifetime in seconds and lifetime in kilobytes of data.



### Note

The reauthentication fails if there is no user at the other end of the connection.

## Examples

The following example shows how to enable reauthentication on rekey for the group policy named FirstGroup:

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

```
hostname(config-group-policy)# re-xauth enable
```

# rip

To enable and change RIP settings, use the **rip** command in global configuration mode. To disable the FWSM RIP routing table updates, use the **no** form of this command.

```
rip if_name {default | passive} [version {1 | 2 [authentication {text | md5} key key_id]}]
```

```
no rip if_name {default | passive} [version {1 | 2 [authentication {text | md5} key key_id]}]
```

## Syntax Description

<b>authentication</b>	(Optional) Enables RIP version 2 authentication.
<b>default</b>	Broadcast a default route on the interface.
<i>if_name</i>	The interface on which RIP is being enabled.
<i>key</i>	Key to authenticate RIP updates.
<i>key_id</i>	Key identification value; valid values range from 1 to 255.
<b>md5</b>	Uses MD5 for RIP message authentication.
<b>passive</b>	Enables passive RIP on the interface. The interface listens for RIP routing broadcasts and uses that information to populate the routing tables but does not broadcast routing updates.
<b>text</b>	Uses clear text for RIP message authentication (not recommended).
<b>version</b>	(Optional) Specifies the RIP version; valid values are <b>1</b> and <b>2</b> .

## Defaults

RIP is disabled.

If you do not specify a version, RIP version 1 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
Global configuration	•	—	•	—	—

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Usage Guidelines

The **rip** command lets you to enable the sending and receiving of RIP routing updates on an interface. You configure RIP update transmission and reception independently; you can enable transmission only, reception only, or both transmission and reception on each interface. Use the **passive** keyword with the **rip** command to enable RIP update reception. Use the **default** keyword with the **rip** command to enable the broadcast of a default route. To enable both transmission and reception of RIP updates on an

interface, you must two **rip** commands for the interface, one with the **default** keyword, enabling the sending of RIP routing updates, and one with the **passive** keyword, enabling the interface to receive RIP updates and to populate the routing table with those updates.

**Note**

The FWSM cannot pass RIP updates between interfaces.

If you specify RIP version 2, you can enable neighbor authentication and use MD5-based encryption to authenticate the RIP updates. When you enable neighbor authentication, you must ensure that the *key* and *key\_id* arguments are the same as those used by neighbor devices that provide RIP version 2 updates. The *key* is a text string of up to 16 characters.

Configuring RIP Version 2 registers the multicast address 224.0.0.9 on the respective interface to be able to accept multicast RIP Version 2 updates. When RIP Version 2 is configured in passive mode, the FWSM accepts RIP Version 2 multicast updates with an IP destination of 224.0.0.9. When RIP Version 2 is configured in default mode, the FWSM transmits default route updates using an IP multicast destination of 224.0.0.9. Removing the RIP version 2 commands for an interface unregisters the multicast address from the interface card.

**Note**

Only Intel 10/100 and Gigabit interfaces support multicasting.

RIP is not supported under transparent mode. By default, the FWSM denies all RIP broadcast and multicast packets. To permit these RIP messages to pass through a FWSM operating in transparent mode you must define access list entries to permit this traffic. For example, to permit RIP version 2 traffic through the security appliance, create an access list entry like `access-list myriplist extended permit ip any host 224.0.0.9`. To permit RIP version 1 broadcasts, create an access list entry like `access-list myriplist extended permit udp any any eq rip`. Apply these access list entries to the appropriate interface using the **access-group** command.

**Examples**

The following example shows how to combine version 1 and version 2 commands and list the information with the **show running-config rip** command after entering the **rip** commands. The **rip** commands let you to do the following.

- Enable version 2 passive and default RIP using MD5 authentication on the outside interface to encrypt the key that is used by the FWSM and other RIP peers, such as routers.
- Enable version 1 passive RIP listening on the inside interface of the FWSM.
- Enable version 2 passive RIP listening on the dmz (demilitarized) interface of the FWSM.

```
hostname(config)# rip outside passive version 2 authentication md5 thisisakey 2
hostname(config)# rip outside default version 2 authentication md5 thisisakey 2
hostname(config)# rip inside passive
hostname(config)# rip dmz passive version 2
```

```
hostname# show running-config rip
rip outside passive version 2 authentication md5 thisisakey 2
rip outside default version 2 authentication md5 thisisakey 2
rip inside passive version 1
rip dmz passive version 2
```

The following example shows how to use the version 2 feature that passes the encryption key in text form:

```
hostname(config)# rip out default version 2 authentication text thisisakey 3
hostname# show running-config rip
```

```
rip outside default version 2 authentication text thisisakey 3
```

**Related Commands**

<b>Command</b>	<b>Description</b>
<b>clear configure rip</b>	Clears all RIP commands from the running configuration.
<b>debug rip</b>	Displays debug information for RIP.
<b>show running-config rip</b>	Displays the RIP commands in the running configuration.

# rmdir

To remove the existing directory, use the **rmdir** command in privileged EXEC mode.

```
rmdir [/noconfirm] [flash:]path
```

## Syntax Description

<b>noconfirm</b>	(Optional) Suppresses the confirmation prompt.
<b>flash:</b>	(Optional) Specifies the nonremovable internal Flash, followed by a colon.
<b><i>path</i></b>	(Optional) The absolute or relative path of the directory to remove.

## 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
3.1(1)	Support for this command was introduced.

## Usage Guidelines

If the directory is not empty, the **rmdir** command fails.

## Examples

This example shows how to remove an existing directory named “test”:

```
hostname# rmdir test
```

## Related Commands

Command	Description
<b>dir</b>	Displays the directory contents.
<b>mkdir</b>	Creates a new directory.
<b>pwd</b>	Displays the current working directory.
<b>show file</b>	Displays information about the file system.

# route

To enter a static or default route for the specified interface, use the **route** command in global configuration mode. Use the **no** form of this command to remove routes from the specified interface.

```
route interface_name ip_address netmask gateway_ip [metric]
```

```
no route interface_name ip_address netmask gateway_ip [metric]
```

## Syntax Description

<i>gateway_ip</i>	Specifies the IP address of the gateway router (the next-hop address for this route).  <b>Note</b> The <i>gateway_ip</i> argument is optional in transparent mode.
<i>interface_name</i>	Internal or external network interface name.
<i>ip_address</i>	Internal or external network IP address.
<i>metric</i>	(Optional) The administrative distance for this route. Valid values range from 1 to 255. The default value is 1.
<i>netmask</i>	Specifies a network mask to apply to <i>ip_address</i> .

## Defaults

The *metric* default is 1.

## 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
1.1(1)	This command was introduced.

## Usage Guidelines

Use the **route** command to enter a default or static route for an interface. To enter a default route, set *ip\_address* and *netmask* to **0.0.0.0**, or use the shortened form of **0**. All routes that are entered using the **route** command are stored in the configuration when it is saved.

Create static routes to access networks that are connected outside a router on any interface. For example, the FWSM sends all packets that are destined to the 192.168.42.0 network through the 192.168.1.5 router with this static **route** command.

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

Once you enter the IP address for each interface, the FWSM creates a CONNECT route in the route table. This entry is not deleted when you use the **clear route** or **clear configure route** commands.

If the **route** command uses the IP address from one of the interfaces on the FWSM as the gateway IP address, the FWSM will ARP for the destination IP address in the packet instead of ARPing for the gateway IP address.

### Examples

The following example shows how to specify one default **route** command for an outside interface:

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

The following example shows how to add these static **route** commands to provide access to the networks:

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

### Related Commands

Command	Description
<b>clear configure route</b>	Removes statically configured <b>route</b> commands.
<b>clear route</b>	Removes routes learned through dynamic routing protocols such as RIP.
<b>show route</b>	Displays route information.
<b>show running-config route</b>	Displays configured routes.

# route-map

To define the conditions for redistributing routes from one routing protocol into another, use the **route-map** command in global configuration mode. To delete a map, use the **no** form of this command.

```
route-map map_tag [permit | deny] [seq_num]
```

```
no route-map map_tag [permit | deny] [seq_num]
```

## Syntax Description

<b>deny</b>	(Optional) Specifies that if the match criteria are met for the route map, the route is not redistributed.
<i>map_tag</i>	Text for the route map tag; the text can be up to 57 characters in length.
<b>permit</b>	(Optional) Specifies that if the match criteria is met for this route map, the route is redistributed as controlled by the set actions.
<i>seq_num</i>	(Optional) Route map sequence number; valid values are from 0 to 65535. Indicates the position that a new route map will have in the list of route maps already configured with the same name.

## Defaults

The defaults are as follows:

- **permit.**
- If you do not specify a *seq\_num*, a *seq\_num* of 10 is assigned to the first route map.

## 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
1.1(1)	This command was introduced.

## Usage Guidelines

The **route-map** command lets you redistribute routes.

The **route-map** global configuration command and the **match** and **set** configuration commands define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has **match** and **set** commands that are associated with it. The **match** commands specify the match criteria that are the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions, which are the redistribution actions to perform if the criteria enforced by the **match** commands are met. The **no route-map** command deletes the route map.

The **match route-map** configuration command has multiple formats. You can enter the **match** commands in any order, and all **match** commands must pass to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** form of the **match** commands removes the specified match criteria.

Use route maps when you want detailed control over how routes are redistributed between routing processes. You specify the destination routing protocol with the **router ospf** global configuration command. You specify the source routing protocol with the **redistribute** router configuration command.

When you pass routes through a route map, a route map can have several parts. Any route that does not match at least one match clause relating to a **route-map** command is ignored; the route is not advertised for outbound route maps and is not accepted for inbound route maps. To modify only some data, you must configure a second route map section with an explicit match specified.

The *seq\_number* argument is as follows:

1. If you do not define an entry with the supplied tag, an entry is created with the *seq\_number* argument set to 10.
2. If you define only one entry with the supplied tag, that entry becomes the default entry for the following **route-map** command. The *seq\_number* argument of this entry is unchanged.
3. If you define more than one entry with the supplied tag, an error message is printed to indicate that the *seq\_number* argument is required.

If the **no route-map map-tag** command is specified (with no *seq-num* argument), the whole route map is deleted (all **route-map** entries with the same *map-tag* text).

If the match criteria are not met, and you specify the **permit** keyword, the next route map with the same *map\_tag* is tested. If a route passes none of the match criteria for the set of route maps sharing the same name, it is not redistributed by that set.

## Examples

The following example shows how to configure a route map in OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

## Related Commands

Command	Description
<b>clear configure route-map</b>	Removes the conditions for redistributing the routes from one routing protocol into another routing protocol.
<b>match interface</b>	Distributes distribute any routes that have their next hop out one of the interfaces specified,
<b>router ospf</b>	Starts and configures an ospf routing process.
<b>set metric</b>	Specifies the metric value in the destination routing protocol for a route map.
<b>show running-config route-map</b>	Displays the information about the route map configuration.

# router ospf

To start an OSPF routing process and configure parameters for that process, use the **router ospf** command in global configuration mode. To disable OSPF routing, use the **no** form of this command.

**router ospf** *pid*

**no router ospf** *pid*

## Syntax Description

*pid* Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535. The *pid* does not need to match the ID of OSPF processes on other routers.

## Defaults

OSPF routing 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
1.1(1)	This command was introduced.

## Usage Guidelines

The **router ospf** command is the global configuration command for OSPF routing processes running on the FWSM. Once you enter the **router ospf** command, the command prompt appears as (config-router)#, indicating that you are in router configuration mode.

When using the **no router ospf** command, you do not need to specify optional arguments unless they provide necessary information. The **no router ospf** command terminates the OSPF routing process specified by its *pid*. You assign the *pid* locally on the FWSM. You must assign a unique value for each OSPF routing process.

The **router ospf** command is used with the following OSPF-specific commands to configure OSPF routing processes:

- **area**—Configures a regular OSPF area.
- **compatible rfc1583**—Restores the method used to calculate summary route costs per RFC 1583.
- **default-information originate**—Generates a default external route into an OSPF routing domain.
- **distance**—Defines the OSPF route administrative distances based on the route type.
- **ignore**—Suppresses the sending of syslog messages when the router receives a link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets.

- **log-adj-changes**—Configures the router to send a syslog message when an OSPF neighbor goes up or down.
- **neighbor**—Specifies a neighbor router. Used to allow adjacency to be established over VPN tunnels.
- **network**—Defines the interfaces on which OSPF runs and the area ID for those interfaces.
- **redistribute**—Configures the redistribution of routes from one routing domain to another according to the parameters specified.
- **router-id**—Creates a fixed router ID.
- **summary-address**—Creates the aggregate addresses for OSPF.
- **timers lsa-group-pacing**—OSPF LSA group pacing timer (interval between group of LSA being refreshed or max-aged).
- **timers spf**—Delay between receiving a change to the SPF calculation.

You cannot configure OSPF when RIP is configured on the FWSM.

### Examples

The following example shows how to enter the configuration mode for the OSPF routing process numbered 5:

```
hostname(config)# router ospf 5
hostname(config-router)#
```

### Related Commands

Command	Description
<b>clear configure router</b>	Clears the OSPF router commands from the running configuration.
<b>show running-config</b> <b>router ospf</b>	Displays the OSPF router commands in the running configuration.

# router-id

To use a fixed router ID, use the **router-id** command in router configuration mode. To reset OSPF to use the previous router ID behavior, use the **no** form of this command.

**router-id** *addr*

**no router-id** [*addr*]

## Syntax Description

*addr* Router ID in IP address format.

## Defaults

If not specified, the highest-level IP address on the FWSM is used as the router ID.

## 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
Router configuration	•	—	•	—	—

## Command History

Release	Modification
1.1(1)	This command was introduced.

## Usage Guidelines

If the highest-level IP address on the FWSM is a private address, then this address is sent in hello packets and database definitions. To prevent this situation, use the **router-id** command to specify a global address for the router ID.

## Examples

The following example sets the router ID to 192.168.1.1:

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

## Related Commands

Command	Description
<b>router ospf</b>	Enters router configuration mode.
<b>show ospf</b>	Displays general information about the OSPF routing processes.