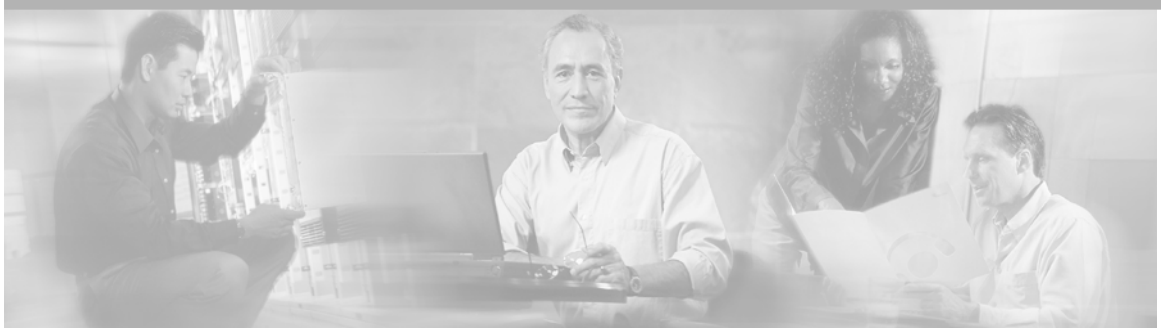

Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference

Firewall Services Module Release 2.3

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-6513-01

Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference

CONTENTS

Preface

This preface describes who should read the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference*, how it is organized, and its document conventions.

Audience

This publication is for experienced network administrators who are responsible for managing network security, configuring firewalls, managing default and static routes, and managing TCP and UDP services.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Using Firewall Services Module Commands	Describes how to use the FWSM commands, command modes, ports, protocols, and deprecated commands.
Chapter 2	Firewall Services Module Commands	Describes the commands used to configure the Firewall Services Module.
Appendix A	Acronyms and Abbreviations	Lists the acronyms and abbreviations used in this reference.
Appendix B	Port and Protocol Values	Lists the port and protocol values.
Index	Index	Index of commands in this publication.

Conventions

This document uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.

Convention	Description
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars. Braces can also be used to group keywords and/or arguments; for example, {**interface** *interface* **type**}.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

The following publications are available for the Firewall Services Module:

- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Installation and Configuration Note*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Software Configuration Guide*
- *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Messages Guide*

Use this document with the FWSM documentation available online at the following site:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/mod_icn/fwsm/fwsm_2_1/index.htm

Cisco provides FWSM technical tips at this URL:

http://www.cisco.com/warp/public/707/index.shtml#FWSM

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

  http://cisco.com/univercd/cc/td/doc/pcat/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Using Firewall Services Module Commands

This chapter describes how to use the Firewall Services Module (FWSM) commands and contains the following sections:

For the definitions of terms and acronyms that are used in this publication, see Appendix A, "Acronyms and Abbreviations."

Using the FWSM Commands

You will use these FWSM commands for basic tasks:

Command	Task
copy running-config	Copies the running configuration from memory. This command is equivalent to the **write memory** command.
copy startup-config	Copies the startup configuration from the flash memory. This command is equivalent to the **write memory** command.
write memory	Saving the configuration.
write terminal	Viewing the configuration.
logging buffered debugging	Accumulating system log (syslog) messages.
show logging	Viewing system log (syslog) messages.
clear logging	Clearing the message buffer.

The FWSM command-line interface (CLI) allows you to do these tasks:

- Check the syntax before entering a command.

  Enter a command and press the **Enter** key to view a quick summary, or precede a command with the **help** command (for example, you can use **help aaa**).

- Abbreviate commands.

  You can use the **config t** command to start configuration mode, the **write t** command to list the configuration, and the **write m** command to write to Flash memory. In most commands, you can abbreviate the **show** command as **sh**. This feature is called command completion.

- Make the IP addresses available for access.

  After changing or removing the **alias**, **access-list**, **global, nat**, **outbound**, and **static** commands, enter the **clear xlate** command.

- Review possible port and protocol numbers at the following Internet Assigned Numbers Authority (IANA) websites:

  http://www.iana.org/assignments/port-numbers
  http://www.iana.org/assignments/protocol-numbers

- Create your configuration in a text editor and then cut and paste it into the configuration.

  You can paste in a line at a time or the whole configuration. Always check your configuration after pasting large blocks of text to be sure that all of the text was copied.

For information about how to build your FWSM configuration, refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Installation and Configuration Note*.

Syslog messages are described in the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module System Messages Guide*.

For information about how to use PDM 4.0 for the FWSM, refer to the online Help included in the PDM software (accessed through the PDM application Help button).

FWSM technical documentation is located at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/iaabu/fwsm/

Command Modes

The FWSM contains a command set that is based on Cisco IOS technologies and provides configurable command privilege modes that are based on the following command modes:

- Unprivileged mode

  Unprivileged mode allows you to see the FWSM settings. The unprivileged mode prompt appears as follows when you first access the FWSM:

  ```
  FWSM>
  ```

- Privileged mode

  Privileged mode allows you to change current settings. Any unprivileged mode command will work in privileged mode. Enter the **enable** command to start the privileged mode from unprivileged mode as follows:

  ```
  FWSM> enable
  Password:
  fwsm#
  ```

The "#" prompt is displayed.

Enter the **exit** or **quit** commands to exit privileged mode and return to unprivileged mode as follows:

```
fwsm# exit

Logoff

Type help or '?' for a list of available commands.
```

Enter the **disable** command to exit privileged mode and return to unprivileged mode as follows:

```
fwsm# disable
fwsm>
```

- Configuration mode

  Configuration mode allows you to change the FWSM configuration. All privileged, unprivileged, and configuration commands are available in this mode. Enter the **configure terminal** command to start the configuration mode as follows:

  ```
  fwsm# configure terminal
  fwsm(config)#
  ```

  Enter the **exit** or **quit** commands to exit configuration mode and return to privileged mode as follows:

  ```
  fwsm(config)# quit
  fwsm#
  ```

  Enter the **disable** command to exit configuration mode and return to unprivileged mode as follows:

  ```
  fwsm(config)# disable
  fwsm>
  ```

- Subconfiguration modes

  When you are in context subconfiguration mode, the prompt changes as follows:

  ```
  fwsm(config-context)#
  ```

  When you are in class subconfiguration mode, the prompt changes as follows:

  ```
  fwsm(config-class)#
  ```

  When you change to a context, the prompt changes as follows:

  ```
  fwsm/context_name#
  ```

  When you are in context configuration mode, the prompt changes as follows:

  ```
  fwsm/context_name(config)#
  ```

CHAPTER 2

Firewall Services Module Commands

This chapter contains an alphabetical listing of all the commands that are available to configure the Firewall Services Module (FWSM) on the Catalyst 6500 series switch and Cisco 7600 series router.

aaa accounting

To include or exclude TACACS+ or RADIUS user accounting on a server (designated by the **aaa-server** command), use the **aaa accounting** command. To disable accounting services, use the **no** form of this command.

[**no**] **aaa accounting** {**include** | **exclude**} *service interface_name source_ip source_mask* [*destination_ip destination_mask*] *server_tag*

Syntax Description

include	Creates a new rule with the specified service to include.
exclude	Creates an exception to a previously stated rule by excluding the specified service from accounting.
service	Accounting service; valid values are **any**, **ftp**, **http**, **telnet**.
interface_name	Interface name from which users require authentication.
source_ip	IP address of the local host or network of hosts that you want to be authenticated or authorized.
source_mask	Network mask of *source_ip*.
destination_ip	(Optional) IP address of the destination hosts that you want to access the *source_ip* address; **0** indicates that all hosts have access.
destination_mask	(Optional) Network mask of the *destination_ip*.
server_tag	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The *interface_name* must match the VLAN number.

Before you can use this command, you must first designate an AAA server with the **aaa-server** command.

To enable accounting for traffic that is specified by an access list, use the **aaa accounting match** command.

User accounting services can track the network services that a user accesses. These records are also kept on the designated AAA server. Accounting information is sent only to the active server in a server group.

When specifying the *service*, use the **any** keyword to provide accounting for all TCP services. For UDP services, use *protocol/port.* The port refers to the TCP or UDP destination port. A port value of 0 (zero) indicates all ports. For protocols other than TCP and UDP, the *port* is not applicable and should not be used. See Appendix B, "Port and Protocol Values" for port information.

Use the **aaa accounting** command with the **aaa authentication** and optionally, the **aaa authorization** commands. You must have authentication for traffic that you want to track.

To track connections from any host, enter the local IP address and netmask as **0.0.0.0 0.0.0.0** or **0 0**. Use the same convention for the destination host IP addresses and netmasks; enter **0.0.0.0 0.0.0.0** to indicate any destination host.

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

Use *interface_name* with the *source_ip* address and the *destination_ip* address to determine where access is to come from and from whom.

Examples

This example shows how to specify that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group:

```
fwsm/context(config)#  aaa accounting include any inside 0 0 0 0
```

Related Commands

aaa accounting match
aaa authentication
aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa accounting match

To enable accounting for traffic that is identified by an access list, use the **aaa accounting match** command. To disable accounting for traffic that is identified by an access list, use the **no** form of this command.

[**no**] **aaa accounting match** *access_list_name interface_name server_tag*

Syntax Description

access_list_name	Access list name.
interface_name	Interface name from which users require authentication.
server_tag	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The *access_list_name* is defined by the **access-list extended** command.

In an ACL, permit = account and deny = do not account.

The AAA server group tag is defined by the **aaa-server** command. Before you can use this command, you must first designate an AAA server with the **aaa-server** command.

Examples

This example shows how to enable accounting on a specific access list:

```
fwsm/context(config)# aaa accounting match acl1 termite scram
fwsm/context(config)# show acl
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
alert-interval 300
```

Related Commands

aaa authentication
aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa authentication

To include or exclude user authentication for traffic through the FWSM, use the **aaa authentication** command. To disable user authentication, use the **no** form of this command.

[**no**] **aaa authentication** {**include** | **exclude** | **https**} *authen_service interface_name source_ip source_mask* [*destination_ip destination_mask*] *server_tag*

Syntax Description

include	Specifies that you want to authenticate the traffic.
exclude	Exempts the traffic from being authenticated.
https	Enables authentication for HTTPS clients only. **Note** This keyword is used without the **aaa authentication secure-http-client** command.
authen_service	Type of traffic to include or exclude from authentication based on the service keyword selected. See Appendix B, "Port and Protocol Values" for valid services.
interface_name	Interface name from which users require authentication.
source_ip	IP address of the host or network of hosts that you want to be authenticated.
source_mask	Network mask of *source_ip*.
destination_ip	(Optional) IP address of the hosts that you want to access the *source_ip* address; **0** indicates all hosts.
destination_mask	(Optional) Network mask of *destination_ip*.
server_tag	AAA server group tag identified by the **aaa-server** command.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For each IP address, one **aaa authentication** command is permitted for inbound connections and one **aaa authentication** command is permitted for outbound connections. A given IP address initiates connections in one direction only.

The **aaa authentication** command enables or disables the following features:

- A host whose IP address is identified by the **aaa-server** command, starts a connection through FTP, Telnet, HTTP or HTTPS, and is prompted for a username and password. If the username and password are verified by the designated TACACS+ or RADIUS authentication server, the FWSM allows further traffic between the authenticating host and the destination address.

The prompts differ between the three services that can access the FWSM for authentication as follows:

- A Telnet user sees a prompt that is generated by the FWSM. The FWSM permits a user up to four tries to log in. If the username or password still fails, the FWSM drops the connection. You can change this prompt with the **auth-prompt** command.
- An FTP user sees a prompt from the FTP program. If a user enters an incorrect password, the connection is dropped immediately.

  If the username or password on the authentication database differs from the username or password on the remote host that you are accessing with FTP, enter the username and password in these formats:

  authentication_user_name@*remote_system_user_name*
  authentication_password@*remote_system_password*

  If you daisy-chain the FWSM, Telnet authentication works in the same way as a single module. For FTP and HTTP authentication, the user has to enter each password and username with an additional at "@" character and password or username for each daisy-chained system. A user can exceed the 63-character password limit depending on how many units are daisy-chained and the password length.

  Some FTP graphical user interfaces (GUIs) do not display challenge values.
- An HTTP user sees a pop-up window that is generated by the browser. If a user enters an incorrect password, the user is prompted again. When the web server and the authentication server are on different hosts, you can use the **virtual** command to get the correct authentication.

The FWSM supports authentication usernames up to 127 characters and passwords up to 16 characters (some AAA servers accept passwords up to 32 characters). A password or username cannot contain an "@" character as part of the password or username string.

The valid values for the access *authen_service* argument are as follows:

- **telnet** —Telnet access
- **ftp**—FTP access
- **http**—HTTP access
- **any**—All services
- *service*/*port*—When you specify a *port*, only the traffic with a matching destination port is included or excluded for authentication. The **tcp/0** optional keyword enables authentication for all TCP traffic, which includes FTP, Telnet, HTTP, and HTTPS.

Note FTP, Telnet, and HTTP are equivalent to **tcp/21**, **tcp/23**, and **tcp/80, https/443**.

Note Only Telnet, FTP, or HTTP traffic triggers interactive user authentication.

If you specify **ip**, all IP traffic is included or excluded for authentication, depending on whether you specify **include** or **exclude**. When all IP traffic is included for authentication, the following occurs:

- Before a user (source IP-based) is authenticated, an FTP, Telnet, HTTP, or HTTPS request triggers authentication and all other IP requests are denied.
- After a user is authenticated through FTP, Telnet, HTTP, HTTPS, or virtual Telnet authentication (see the **virtual** command), all traffic is free from authentication until the **uauth** timeout.

Use *interface_name*, *source_ip*, and *destination_ip* to define where access is to come from and from whom. The address for *source_ip* is always on the highest security level interface, and *destination_ip* is always on the lowest security level interface.

The maximum username prompt for HTTP authentication is 30 characters. The maximum password length is 15 characters.

The **aaa authentication** command is not intended to mandate your security policy. The authentication servers determine whether a user can or cannot access the system. The FWSM interacts with FTP, HTTP (Web access), HTTPS, and Telnet to display the credential prompts for logging in to the network or logging in to exit the network.

HTTP Authentication

The **aaa authentication** command supports HTTP authentication.

Caution We do not recommend that you enable AAA authentication for FTP, Telnet, HTTP, or HTTPS and share the same AAA server for authenticating inbound and outbound connections.

When using HTTP authentication to a site running Microsoft IIS that has "Basic text authentication" or "NT Challenge" enabled, you may be denied access from the Microsoft IIS server. This situation occurs because the browser appends the string: "Authorization: Basic=Uuhjksdkfhk==" to the HTTP GET commands. This string contains the FWSM authentication credentials.

Windows NT Microsoft IIS servers respond to the credentials and assume that a Windows NT user is trying to access privileged pages on the server. Unless the FWSM username password combination is exactly the same as a valid Windows NT username and password combination on the Microsoft IIS server, the HTTP GET command is denied.

To solve this problem, the FWSM provides the **virtual http** command, which redirects the browser's initial connection to another IP address, authenticates the user, and then redirects the browser back to the URL to which the user originally requested.

Once authenticated, a user does not have to reauthenticate even if the FWSM uauth timeout is set low because the browser caches the "Authorization: Basic=Uuhjksdkfhk==" string in every subsequent connection to that particular site. This string can *only* be cleared when the user exits *all* instances of Netscape Navigator or Internet Explorer and restarts. Flushing the cache does not clear the string.commands.

If the user repeatedly browses the Internet, the browser resends the "Authorization: Basic=Uuhjksdkfhk==" string to transparently reauthenticate the user.

Multimedia applications, such as CU-SeeMe, Intel Internet Phone, MeetingPoint, and MS Netmeeting silently start the HTTP service.

Note To avoid interfering with these applications, do not enter blanket outgoing **aaa** commands for all challenged ports (such as using the **any** optional keyword). Be selective with which ports and addresses that you use to challenge HTTP and when you set the user authentication timeouts to a higher timeout value. Otherwise, the multimedia programs may fail and crash the PC after establishing outgoing sessions from the inside sessions.

TACACS+ and RADIUS Servers

Up to 256 TACACS+ or RADIUS servers are permitted (up to 16 servers in each of the up to 16 server groups). You can set the number of servers by using the **aaa-server** command. When a user logs in, the servers are accessed one at a time starting with the first server that you specify in the configuration, until a server responds.

The FWSM permits only one authentication type per network. For example, if one network connects through the FWSM using TACACS+ for authentication, another network connecting through the FWSM can authenticate with RADIUS. One network cannot authenticate with both the TACACS+ and RADIUS servers.

For the TACACS+ server, if you do not specify a key to the **aaa-server** command, no encryption occurs.

The FWSM displays the same timeout message for both the RADIUS and TACACS+ servers. The message "aaa server host machine not responding" displays when either of the following occurs:

- The AAA server system is down.
- The AAA server system is up, but the service is not running.

Examples

This example shows how to authenticate traffic:

```
fwsm/context(config)#  aaa authentication include any 172.31.0.0 255.255.0.0 0.0.0.0
0.0.0.0 tacacs+
```

This example shows how to prevent authentication on traffic:

```
fwsm/context(config)#  aaa authentication exclude telnet 172.31.38.0 255.255.255.0 0.0.0.0
0.0.0.0 tacacs+
```

This example demonstrates how to use the *interface_name* argument. The firewall has an inside network of 192.168.1.0, an outside network of 209.165.201.0 (subnet mask 255.255.255.224), and a perimeter network of 162.65.20.28 (subnet mask 255.255.255.224).

This example shows how to enable authentication for connections that originated from the inside network to the outside network:

```
fwsm/context(config)#  aaa authentication include any 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example shows how to enable authentication for connections that originated from the inside network to the perimeter network:

```
fwsm/context(config)#  aaa authentication include any 192.168.1.0 255.255.255.0
162.65.20.28 255.255.255.224 tacacs+
```

This example shows how to enable authentication for connections that originated from the outside network to the inside network:

```
fwsm/context(config)#  aaa authentication include any 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

This example shows how to enable authentication for connections that originated from the outside network to the perimeter network:

```
fwsm/context(config)#  aaa authentication include any 209.165.201.0 255.255.255.224
162.65.20.28 255.255.255.224 tacacs+
```

This example shows how to enable authentication for connections that originated from the perimeter network to the outside network:

```
fwsm/context(config)#  aaa authentication include any 162.65.20.28 255.255.255.224
209.165.201.0 255.255.255.224 tacacs+
```

This example specifies that IP addresses 10.0.0.1 through 10.0.0.254 can originate outbound connections and then shows how to enable user authentication so that those addresses must enter user credentials to exit the firewall. The first **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The second **aaa authentication** command lets host 10.0.0.42 start outbound connections without being authenticated. The default authentication group is **tacacs+**.

```
fwsm/context(config)#  nat (inside) 1 10.0.0.0 255.255.255.0
fwsm/context(config)#  aaa authentication include any 0 0 tacacs+
fwsm/context(config)#  aaa authentication exclude 10.0.0.42 255.255.255.255 tacacs+ any
```

This example shows how to permit inbound access to any IP address in the range of 209.165.201.1 through 209.165.201.30 indicated by the 209.165.201.0 network address (subnet mask 255.255.255.224). All services are permitted by the **access-list** command. The **aaa authentication** command permits authentication on FTP, HTTP, or Telnet depending on what the authentication server handles. The authentication server is at IP address 10.16.1.20 on the inside interface.

```
fwsm/context(config)#  aaa-server AuthIn protocol tacacs+
fwsm/context(config)#  aaa-server AuthIn (inside) host 10.16.1.20 thisisakey timeout 20
fwsm/context(config)#  static (inside,outside) 209.165.201.0 10.16.1.0 netmask
255.255.255.224
fwsm/context(config)#  access-list acl_out permit tcp 10.16.1.0 255.255.255.0
209.165.201.0 255.255.255.224
fwsm/context(config)#  access-group acl_out in interface outside
fwsm/context(config)#  aaa authentication include any 0 0 AuthIn
```

This example shows how to enable HTTPS authentication for a client:

```
fwsm/context(config)# aaa authentication secure-http-client
fwsm/context(config)# aaa authentication include http int3 0000 aaaserver3
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa authentication console

To enable authentication for access to the FWSM CLI, use the **aaa authentication console** command. To disable authentication verification, use the **no** form of this command.

[**no**] **aaa authentication** {**enable | telnet | ssh | http**} **console** {*server_tag* [**LOCAL**] | **LOCAL**}

Syntax Description

enable	(Optional) Specifies access verification for the FWSM's privileged mode.
telnet	(Optional) Specifies access verification for the Telnet access to the FWSM console.
ssh	(Optional) Specifies access verification for the SSH access to the FWSM console.
http	(Optional) Specifies access verification for the HTTP (Hypertext Transfer Protocol) access to the FWSM (through FDM).
server_tag	AAA server group tag of the local database.
LOCAL	See the "Usage Guidelines" section for information.

Defaults

The defaults are as follows:

- The login password is **cisco**.

Note The **cisco** password cannot be used when specifying a password for user authentication.

- The enable password is not set.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support fallback to LOCAL.

Usage Guidelines

The AAA server group tag is defined by the **aaa-server** command.

The **LOCAL** keyword specifies a second authentication method that can be local only. The **LOCAL** keyword is optional when specified as a RADIUS or TACACS+ server only.

Any access to the module (SSH, Telnet, enable) requiring a username and password is prompted only three times.

- The **enable** and **ssh** keywords allow three tries before stopping with an access-denied message as follows:
  - The **enable** keyword requests a username and password before accessing privileged mode.
  - The **ssh** keyword requests a username and password before the first command line prompt on the SSH console connection. The **ssh** keyword allows a maximum of three authentication attempts.
- The **telnet** keyword prompts you continually until you successfully log in. The **telnet** keyword forces you to specify a username and password before the first command line prompt of a Telnet console connection.

Telnet access to the FWSM CLI is available from any internal interface and from the outside interface with IPSec configured. Telnet access requires previous use of the **telnet** command.

SSH access to the FWSM console is also available from any interface (IPSec does not have to be configured on the interface). SSH access requires previous use of the **ssh** command.

If an **aaa authentication ssh console** *server_tag* command is not defined, you can gain access to the CLI with the username **pix** and with the FWSM Telnet password (set with the **passwd** command). If the **aaa** command is defined but the SSH authentication requests timeouts, which implies that the AAA servers may be down or not available, you can gain access to the FWSM using the **PIX** username and the enable password (set with the **enable password** command).

The FWSM supports authentication usernames up to 127 characters and passwords up to 16 characters (some AAA servers accept passwords up to 32 characters). A password or username may not contain an "@" character as part of the password or username string.

The command only accepts the second, optional **LOCAL** keyword when the *server_tag* refers to an existing, valid TACACS+ or RADIUS server group defined in a **aaa-server** command. You can configure **LOCAL** as the first and only *server_tag*.

The **no** form of the command removes the complete command and does not support removing single methods.

Examples

This example shows how to enable authentication service for the FWSM console:

```
fwsm/context(config)# aaa authentication enable console 756
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa authentication match

To enable authentication on a specific access list, use the **aaa authentication match** command. To disable authentication on a specific access list, use the **no** form of this command.

[**no**] **aaa authentication match** *access_list_name interface_name server_tag*

Syntax Description

access_list_name	Access list name.
interface_name	Interface name.
server_tag	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The *access_list_name* is defined by the **access-list deny-flow-max** command.

The AAA server group tag is defined by the **aaa-server** command. Enter **TACACS+** or **RADIUS** to use the authentication database.

The FWSM supports authentication usernames up to 127 characters and passwords up to 16 characters (some AAA servers accept passwords up to 32 characters). A password or username may not contain an "@" character as part of the password or username string.

Examples

This example shows how to enable authentication on a specific access list:

```
fwsm/context(config)#  aaa authentication match
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa authentication secure-http-client

To enable encryption of usernames and passwords that are exchanged between an HTTP client and the FWSM, use the **aaa authentication secure-http-client** command. To disable encryption for usernames and passwords, use the **no** form of this command.

[**no**] **aaa authentication secure-http-client**

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to enable authentication on a specific access list:

```
fwsm/context(config)#  aaa authentication secure-http-client
fwsm/context(config)#  show aaa
aaa authentication secure-http-client
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
show aaa
ssh
telnet
virtual

aaa authorization

To include or exclude a service from authorization to the specified host, use the **aaa authorization** command. To disable the feature, use the **no** form of this command.

[**no**] **aaa authorization** {**include** | **exclude**} *service interface_name source_ip source_mask destination_ip destination_mask tacacs_server_tag*

Syntax Description

include	Creates a new rule with the specified service to include.
exclude	Creates an exception to a previously stated rule by excluding the specified service from authorization to the specified host.
service	Services that require authorization; see the "Usage Guidelines" section for more information.
interface_name	Interface name that requires authentication.
source_ip	IP address of the host or the network of hosts that you want to be authorized.
source_mask	Network mask of the *source_ip*.
destination_ip	IP address of the hosts that you want to access the *source_ip* address.
destination_mask	Network mask of the *destination_ip*.
tacacs_server_tag	TACACS+ server group tag.

Defaults

An IP address of **0** indicates all hosts.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support a second LOCAL method for AAA configurations.

Usage Guidelines

The **exclude** keyword replaces the former **except** optional keyword by allowing the user to specify a port to exclude to a specific host or hosts.

When specifying the destination IP, use 0 to indicate all hosts.

For the destination and local mask, always specify a specific mask value. Use **0** if the IP address is 0, and use **255.255.255.255** for a host. Always specify a specific mask value.

Use *interface_name* in combination with the *source_ip* address and the *destination_ip* address to determine where access is to come from and from whom. The *source_ip* address is always on the highest security level interface and *destination_ip* is always on the lowest security level.

You can set the local IP address to **0** to indicate all hosts and to let the authentication server decide which hosts are authenticated.

Valid values for *service* are **any**, **ftp**, **http**, **telnet**, or *protocol/port*. Services that are not specified are authorized implicitly. Services that are specified in the **aaa authentication** command do not affect the services that require authorization.

For *protocol/port*, enter the following:

- *protocol*—Enter the protocol (**6** for TCP, **17** for UDP, **1** for ICMP, and so on).
- *port*—Enter the TCP or UDP destination port or port range. The *port* can also be the ICMP type; that is, 8 for ICMP echo or ping. A port value of 0 (zero) means all ports. Port ranges apply only to the TCP and UDP protocols, not to ICMP. For protocols other than TCP, UDP, and ICMP, the *port* is not applicable and should not be used. An example port specification is as follows:

  ```
  fwsm#/context(config)# aaa authorization include udp/53-1024 inside 0 0 0 0
  ```

  This example shows how to enable authorization for DNS lookups to the inside interface for all clients and authorizes access to any other services that have ports in the range of 53 to 1024.

A specific authorization rule does not require the equivalent authentication. Authentication is only required with either FTP, HTTP, or Telnet to provide an interactive method with the user to enter the authorization credentials.

Except for its use with command authorization, the **aaa authorization** command requires previous configuration with the **aaa authentication** command; however, use of the **aaa authentication** command does not require use of the **aaa authorization** command.

Currently, the **aaa authorization** command is supported for use with local and TACACS+ servers but not with RADIUS servers. Although explicit RADIUS authorization cannot be configured, a dynamic ACL can be set at the RADIUS server to provide authorization (even if it is not configured in the FWSM).

Tip The **help aaa** command displays the syntax and usage for the **aaa authentication**, **aaa authorization**, **aaa accounting**, and **aaa proxy-limit** commands in summary form.

One **aaa authorization** command is permitted for each IP address. To authorize more than one service with **aaa authorization**, use the **any** keyword for the service type.

If the first authorization attempt fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. This example shows an authorization timeout message in Telnet:

```
Unable to connect to remote host: Connection timed out
```

User authorization services control which network services that a user can access. After a user is authenticated, attempts to access restricted services cause the FWSM to verify the access permissions of the user with the designated AAA server.

Note RADIUS authorization is supported for use with the **access-list deny-flow-max** commands and for use in configuring a RADIUS server with an **acl=***access_list_name* vendor-specific identifier. For more information, see the **access-list deny-flow-max** command and the **aaa-server radius-authport** command.

If the AAA console login request times out, you can gain access to the FWSM by entering the **fwsm** username and the enable password.

When specifying the services *service* option, the valid values are **telnet**, **ftp**, **http**, **https**, **tcp** or **0**, **tcp** or *port*, **udp** or *port*, **icmp** or *port* or *protocol* [/*port*]. Only the Telnet, FTP, HTTP, and HTTPS traffic triggers user interactive authentication.

For authentication of console access, Telnet access, SSH access, and enable mode access, specify **telnet**, **ssh**, or **enable**.

Examples

This example shows how to specify the default FWSM protocol configuration:

```
fwsm/context(config)#  aaa-server TACACS+ protocol tacacs+
fwsm/context(config)#  aaa-server RADIUS protocol radius
fwsm/context(config)#  aaa-server LOCAL protocol local
```

This example shows how to use the default protocol TACACS+ with the **aaa** commands. The first command specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three commands specify that any users starting outbound connections to any destination host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command specifies that access to the FWSM requires authentication from the TACACS+ server.

```
fwsm/context(config)#  aaa-server TACACS+ (inside) host 10.1.1.10 the key timeout 20
fwsm/context(config)#  aaa authentication include any 0 0 0 0 TACACS+
fwsm/context(config)#  aaa authorization include any 0 0 0 0
fwsm/context(config)#  aaa accounting include any 0 0 0 0 TACACS+
fwsm/context(config)#  aaa authentication TACACS+
```

This example shows how to enable authorization for DNS lookups from the outside interface:

```
fwsm/context(config)#  aaa authorization include udp/53 0.0.0.0 0.0.0.0
```

This example shows how to enable authorization of ICMP echo-reply packets arriving at the inside interface from inside hosts:

```
fwsm/context(config)#  aaa authorization include 1/0 0.0.0.0 0.0.0.0
```

Users will not be able to ping external hosts if they have not been authenticated using Telnet, HTTP, or FTP.

This example shows how to enable authorization only for ICMP echoes (pings) that arrive at the inside interface from an inside host:

```
fwsm/context(config)#  aaa authorization include 1/8 0.0.0.0 0.0.0.0
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa authorization command

To enable authorization for a local or a TACACS server, use the **aaa authorization command** command. To disable authorization for local or a TACACS server, use the **no** form of this command.

[**no**] **aaa authorization command** {*LOCAL_server_tag* | *tacacs_server_tag*}

Syntax Description

LOCAL_server_tag	Predefined server tag for the AAA local protocol.
tacacs_server_tag	Predefined server tag for the TACACS user authentication server.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support a second LOCAL method for AAA configurations.

Usage Guidelines

You can enter the *LOCAL_server_tag* argument for the group tag value and use the local FWSM database AAA services such as local command authorization privilege levels.

Examples

This example shows how to enable authorization for a local or a TACACS server:

```
fwsm/context(config)# aaa authorization Server1
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa authorization match

To enable the local or TACACS+ user-authorization services for a specific **access-list** command name, use the **aaa authorization match** command. To disable the feature, use the **no** form of this command.

[**no**] **aaa authorization match** *access_list_name interface_name server_tag*

Syntax Description

access_list_name	**access-list** command name.
interface_name	Interface name that requires authentication.
server_tag	AAA server group tag as defined by the **aaa-server** command.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support a second LOCAL method for AAA configurations.

Usage Guidelines

The AAA server group tag is defined by the **aaa-server** command. Enter **TACACS+** or **RADIUS** to use the authentication database.

The *access_list_name* is defined by the **access-list deny-flow-max** command.

The FWSM supports authentication usernames up to 127 characters and passwords up to 16 characters (some AAA servers accept passwords up to 32 characters). A password or username may not contain an "@" character as part of the password or username string.

Examples

This example shows how to enable authorization for a specified access list:

```
fwsm/context(config)# aaa authorization match my_access inside Server2
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service

ssh
telnet
virtual

aaa proxy-limit

To specify the number of concurrent proxy connections that are allowed per user, use the **aaa proxy-limit** command.

[**no**] **aaa proxy-limit** {*proxy_limit* | **disable**}

Syntax Description

proxy_limit	Number of concurrent proxy connections allowed per user; valid values are from 1 to 128.
disable	Disables the proxy limit.

Defaults

The *proxy_limit* is 16.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **aaa proxy-limit** command enables you to manually configure the uauth session limit by setting the maximum number of concurrent proxy connections that are allowed per user.

An uauth session is a cut-through session that performs authentication or authorization (the connection is proxied).

If a source address is a proxy server, you should exclude this IP address from authentication or increase the number of allowable outstanding AAA requests.

Examples

This example shows how to set and display the maximum number of outstanding authentication requests allowed:

```
fwsm/context(config)#  aaa proxy-limit 6
fwsm/context(config)#  show aaa proxy-limit
aaa proxy-limit 6
```

Related Commands

aaa authentication
aaa authorization
aaa-server
show aaa proxy-limit

aaa-server

To define the AAA server group, use the **aaa-server** command. To remove the AAA server group, use the **no** form of this command.

[**no**] **aaa-server** *server_tag*

[**no**] **aaa-server** *server_tag* **max-failed-attempts** *tries*

[**no**] **aaa-server** *server_tag* **deadtime** *deatimeout*

aaa-server *server_tag* [*interface_name*] **host** *server_ip* [*key*] [**timeout** *seconds*]

aaa-server *server_tag* **protocol** *auth_protocol* **tacacs+** | **radius**

Syntax Description

server_tag	Alphanumeric string that is the name of the server group.
max-failed-attempts *tries*	Specifies the maximum number of AAA requests to attempt to each AAA server in an AAA server group; the range is from 1 to 5 counters.
deadtime *deatimeout*	Specifies the number of minutes to declare the AAA server group as unresponsive; the range is from 0 to 1440 minutes.
interface_name	(Optional) Interface name on which the server resides.
host *server_ip*	(Optional) IP address of the TACACS+ or RADIUS server.
key	(Optional) Case-sensitive, alphanumeric keyword up to 127 characters and is the same value as the key on the TACACS+ server.
timeout *seconds*	(Optional) Retransmit timer that specifies the time duration before the FWSM chooses the next AAA server.
protocol *auth_protocol*	Type of AAA server, either **tacacs+** or **radius**.

Defaults

The defaults are as follows:

- The FWSM listens for RADIUS on ports 1645 for authentication and 1646 for accounting. The default ports are defined in RFC 2058 as 1812 for authentication and 1813 for accounting. The FWSM RADIUS ports were not changed for backward-compatibility purposes.
- The following are the **aaa-server** default protocols:
  - aaa-server TACACS+ protocol tacacs+
  - aaa-server RADIUS protocol radius
  - aaa-server LOCAL protocol local
- The default timeout value is 10 seconds.
- The interface name *interface_name* defaults to the outside.
- The **max-attempts** is 3.
- The **deadtime** is 10.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support a second LOCAL method for AAA configurations.

Usage Guidelines

The **aaa-server** command allows you to specify AAA server groups. The FWSM lets you define separate groups of TACACS+ or RADIUS servers for specifying different types of traffic. For example, you can specify a TACACS+ server for inbound traffic and another for outbound traffic. You can also specify that all outbound HTTP traffic will be authenticated by a TACACS+ server and that all inbound traffic will use RADIUS. The **aaa-server** command is used with the **crypto map** command to establish an authentication association so that VPN clients are authenticated when they access the FWSM.

Certain types of AAA services can be directed to different servers. Services can also be set up to fail over to multiple servers.

Use the *server_tag* in the **aaa** command to associate **aaa authentication** and **aaa accounting** commands to an AAA server. Up to 14 server groups are permitted. However, you cannot use the **LOCAL** keyword with the **aaa-server** command because the keyword is predefined by the FWSM.

Other **aaa** commands reference the server tag group defined by the **aaa-server** command *server_tag* parameter. This global setting takes effect when the TACACS+ or RADIUS service is started.

Note When a cut-through proxy is configured, TCP sessions (Telnet, FTP, HTTP, or HTTPS) may have their sequence number randomized even if the **norandomseq** optional keyword is used in the **nat** or **static** command. This situation occurs when an AAA server proxies the TCP session to authenticate the user before permitting access.

AAA server groups are defined by a tag name that directs different types of traffic to each authentication server. If the first authentication server in the list fails, the AAA subsystem fails over to the next server in the tag group. You can have up to 14 tag groups, and each group can have up to 14 AAA servers for a total up to 196 AAA servers.

The **max-attempts** *number* keyword and argument allow you to configure the number of AAA requests to an AAA server before declaring that server unresponsive and tries the next server in the group. You should set the **max-attempts** *number* keyword and argument and the timeout values for the fall-back behavior when authenticating or authorizing commands in a fall-back configuration. For example, if you want to declare an individual AAA server as unresponsive, you should reduce the **max-attempts** *number* setting to **1** or **2**.

You can configure the **deadtime** *minutes* keyword and argument without having configured the LOCAL method on any of the **authentication** and **authorization** commands. The **deadtime** *minutes* keyword and argument affect only the operations when you configure two methods for authenticating and authorizing AAA.

Note The second method must be LOCAL.

The **deadtime** *minutes* keyword and argument specify the minutes that a particular authentication or authorization method should be marked as unresponsive and skipped. When a AAA server group is marked unresponsive, the FWSM immediately performs the authentication or authorization against the next method specified (which is the local FWSM user database).

Note Every server in a group must be marked unresponsive before the whole group is declared unresponsive.

When you configure the deadtime to 0, the AAA server group is not considered unresponsive and all authentication and authorization requests are always attempted against this AAA server group before using the next method in the method list.

The **no** form of the **deadtime** command restores the command to its default value of 10 minutes.

The deadtime period begins as soon as the last server in the AAA server group has been marked as down (unresponsive). A server is marked as down when the max-attempts value is reached and AAA fails to receive a response. When the deadtime period expires, the AAA server group is active and all requests are submitted again to the AAA servers in the AAA server group.

Some AAA servers accept passwords up to 32 characters, but the FWSM allows passwords up to 16 characters only.

When specifying the key, any characters entered past 127 are ignored. The key is used between the client and server for encrypting data between them. The key must be the same on both the client and server systems. Spaces are not permitted in the key, but other special characters are permitted in the key.

The timeout default is 10 seconds. The maximum time is 30 seconds. If the timeout value is 10 seconds, the FWSM retransmits for 10 seconds. If no acknowledgment is received, the FWSM tries three times more for a total of 40 seconds to retransmit data before the next AAA server is selected.

If accounting is enabled, the accounting information goes only to the active server.

If you are upgrading from a previous version of FWSM and have **aaa** commands in your configuration, using the default server groups lets you maintain backward compatibility with the **aaa** commands in your configuration.

The previous server type optional keyword at the end of the **aaa authentication** and **aaa accounting** commands has been replaced with the **aaa-server** *server_tag* group name.

This example shows how to use the default protocol TACACS+ with the **aaa** commands:

```
fwsm/context(config)#  aaa-server TACACS+ (inside) host 10.1.1.10 thekey timeout 20
fwsm/context(config)#  aaa authentication include any 0 0 0 0 TACACS+
fwsm/context(config)#  aaa authorization include any outbound 0 0 0 0 host 10.1.1.10
fwsm/context(config)#  aaa accounting include any 0 0 0 0 TACACS+
fwsm/context(config)#  aaa authentication TACACS+
```

The previous example specifies that the authentication server with the IP address 10.1.1.10 resides on the inside interface and is in the default TACACS+ server group. The next three commands specify that any users starting outbound connections to any destination host will be authenticated using TACACS+, that the users who are successfully authenticated are authorized to use any service, and that all outbound connection information will be logged in the accounting database. The last command specifies that access to the FWSM requires authentication from the TACACS+ server.

This example creates the AuthOut and AuthIn server groups for RADIUS authentication and specifies that servers 10.0.1.40, 10.0.1.41, and 10.1.1.2 on the inside interface provide authentication. The servers in the AuthIn group authenticate inbound connections, and the AuthOut group authenticates outbound connections.

```
fwsm/context(config)# aaa-server AuthIn protocol radius
fwsm/context(config)# aaa-server AuthIn (inside) host 10.0.1.40 ab timeout 20
fwsm/context(config)# aaa-server AuthIn (inside) host 10.0.1.41 abc timeout 4
fwsm/context(config)# aaa-server AuthOut protocol radius
fwsm/context(config)# aaa-server AuthOut (inside) host 10.1.1.2 abc123 timeout 15
fwsm/context(config)# aaa authentication include any 0 0 0 0 AuthIn
fwsm/context(config)# aaa authentication include any 0 0 0 0 AuthOut
```

This example shows how to list the commands that can be used to establish an Xauth crypto map:

```
fwsm/context(config)# ip address inside 10.0.0.1 255.255.255.0
fwsm/context(config)# ip address outside 168.20.1.5 255.255.255.0
fwsm/context(config)# ip local pool dealer 10.1.2.1-10.1.2.254
fwsm/context(config)# nat (inside) 0 access-list 80
fwsm/context(config)# aaa-server TACACS+ host 10.0.0.2 secret123
fwsm/context(config)# crypto ipsec transform-set pc esp-des esp-md5-hmac
fwsm/context(config)# crypto dynamic-map cisco 4 set transform-set pc
fwsm/context(config)# crypto map partner-map 20 ipsec-isakmp dynamic cisco
fwsm/context(config)# crypto map partner-map client configuration address initiate
fwsm/context(config)# crypto map partner-map client authentication TACACS+
fwsm/context(config)# crypto map partner-map interface outside
fwsm/context(config)# isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
fwsm/context(config)# isakmp client configuration address-pool local dealer outside
fwsm/context(config)# isakmp policy 8 authentication pre-share
fwsm/context(config)# isakmp policy 8 encryption des
fwsm/context(config)# isakmp policy 8 hash md5
fwsm/context(config)# isakmp policy 8 group 1
fwsm/context(config)# isakmp policy 8 lifetime 86400
```

Related Commands

aaa authentication
aaa authorization
aaa-server
show aaa proxy-limit

aaa-server radius-acctport

To set the port number of the RADIUS server that the FWSM uses for accounting functions, use the **aaa-server radius-acctport** command. To return to the default settings, use the **no** form of this command.

[**no**] **aaa-server radius-acctport** [*acct_port*]

Syntax Description

acct_port	(Optional) RADIUS authentication port number; valid values are from 1 to 65535.

Defaults

acct_port is 1645.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can change authorization and accounting port settings on the FWSM with the **aaa-server radius-acctport** and **aaa-server radius-authport** commands. These commands specify the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions.

The default RADIUS accounting port is 1645 and the default RADIUS authorization port is 1646. If your authentication server uses ports other than 1645 and 1646, then you must configure the FWSM for the appropriate ports prior to starting the RADIUS service with the **aaa-server** command. For example, some RADIUS servers use the port numbers 1812 and 1813 as defined in RFC 2138 and RFC 2139. If your RADIUS server uses ports 1812 and 1813, you must use the **aaa-server radius-authport** and **aaa-server radius-acctport** commands to reconfigure the FWSM to use ports 1812 and 1813.

These port pairs are assigned to authentication and accounting services on the RADIUS servers:

- 1645 (authentication), 1646 (accounting)—default for the FWSM
- 1812 (authentication), 1813 (accounting)—alternate

You can see these and other commonly used port number assignments online at this URL:

http://www.iana.org/assignments/port-numbers

See the "Specifying Port Values" section in Appendix B for additional information about port number assignments.

Examples

This example shows how to set the port number of the RADIUS server that the FWSM uses for accounting functions:

```
fwsm/context(config)#  aaa-server radius-acctport
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

aaa-server radius-authport

To set the port number of the RADIUS server that the FWSM uses for authentication functions, use the **aaa-server radius-authport** command. To return to the default settings, use the **no** form of this command.

[**no**] **aaa-server radius-authport** [*auth_port*]

Syntax Description

acct_port	(Optional) RADIUS authentication port number; valid values are from 1 to 65535

Defaults

auth_port is 1646.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can change authorization and accounting port settings on the FWSM with the **aaa-server radius-acctport** and **aaa-server radius-authport** commands. These commands specify the destination TCP/UDP port number of the remote RADIUS server host to which you wish to assign authentication or accounting functions.

The default RADIUS accounting port is 1645 and the default RADIUS authorization port is 1646. If your authentication server uses ports other than 1645 and 1646, then you must configure the FWSM for the appropriate ports prior to starting the RADIUS service with the **aaa-server** command. For example, some RADIUS servers use the port numbers 1812 and 1813 as defined in RFC 2138 and RFC 2139. If your RADIUS server uses ports 1812 and 1813, you must use the **aaa-server radius-authport** and **aaa-server radius-acctport** commands to reconfigure the FWSM to use ports 1812 and 1813.

The following port pairs are assigned to authentication and accounting services on the RADIUS servers:

- 1645 (authentication), 1646 (accounting)—default for the FWSM
- 1812 (authentication), 1813 (accounting)—alternate

You can see these and other commonly used port number assignments online at this URL:

http://www.iana.org/assignments/port-numbers

See the "Specifying Port Values" section in Appendix B for additional information about port number assignments.

Examples

This example shows how to set the port number of the RADIUS server that the FWSM uses for authentication functions:

```
fwsm/context(config)# aaa-server radius-authport
```

Related Commands

aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

access-group

To bind the access list to an interface, use the **access-group** command. To unbind the access list from the interface, use the **no** form of this command.

[**no**] **access-group** *access-list* {**in** | **out**} **interface** *interface_name* [**per-user-override**]

Syntax Description

access-list	Access list *id*.
in	Filters the inbound packets at the specified interface.
out	Filters the outbound packets at the specified interface.
interface *interface_name*	Specifies the name of the network interface.
per-user-override	(Optional) Allows the per-user ACLs downloaded by the Authenticaion, Authorization and Accounting (AAA) configuration to override the existing interface ACLs. Clients must use RADIUS servers for authorization.

Defaults

per-use-override is off..

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.3(1)	Support for the **per-user-override** option was implemented.

Usage Guidelines

The **access-group** command binds an access list to an interface. The **in** keyword applies the access list to the traffic on the specified interface. The **out** keyword applies the access list to the outbound traffic.

The **no access-group** command unbinds the access list from the interface *interface_name*.

The **show access-group** command displays the current access list bound to the interfaces.

The **clear access-group** command removes all the ACLs from the interfaces.

The **access-group per-user-override** command is implemented for only the inbound ACLs and not for the outbound ACLs.

Examples

This example shows how to use the **access-group** command:

```
fwsm/context(config)# static (inside,outside) 209.165.201.3 10.1.1.3
fwsm/context(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
fwsm/context(config)# access-group acl_out in interface outside
```

The **static** command provides a global address of 209.165.201.3 for the web server at 10.1.1.3. The **access-list** command lets any host access the global address using port 80. The **access-group** command specifies that the **access-list** command applies to traffic entering the outside interface.

Related Commands

access-list alert-interval
access-list deny-flow-max
access-list extended
access-list remark
clear access-group
clear access-list
object-group
show access-group
show access-list

access-list alert-interval

To specify the time interval between deny flow maximum messages, use the **access-list alert-interval** command. To return to the default settings, use the **no** form of this command.

[**no**] **access-list alert-interval** *secs*

Syntax Description

secs	Time interval between deny flow maximum message generation; valid values are from 1 to 3600 seconds.

Defaults

300 seconds

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **access-list alert-interval** command sets the time interval for generating the syslog message 106101. The syslog message 106101 alerts you that the FWSM has reached a deny flow maximum. When the deny flow maximum is reached, another 106101 message is generated if at least *secs* seconds have occurred since the last 106101 message.

See the **access-list deny-flow-max** command for information about the deny flow maximum message generation.

Examples

This example shows how to specify the time interval between deny flow maximum messages:

```
fwsm/context(config)# access-list alert-interval 30
```

Related Commands

access-list deny-flow-max
access-list extended
clear access-list
show access-list

access-list commit

To compile and apply access lists when you are in the manual-commit mode, use the **access-list commit** command.

access-list commit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If a context is in access-list mode, newly added rules are not added to the CLS classifier until a **commit** command is issued. Those rules are flagged and added once the **commit** command is entered.

The commit mode provides user-initiated compilation and affects all the commands that are stored as an ACL configuration in the network processor that require a compilation before they are applied. The **access-list commit** command applies to the following commands:

- **aaa authentication** (**include** and **exclude** versions only)
- **aaa authorization** (**include** and **exclude** versions only)
- **aaa accounting** (**include** and **exclude** versions only)
- **aaa access-list** commands
- **established**
- **filter** commands
- **fixup protocol** is affected only by the **commit** command
- **http**
- **icmp**
- **nat 0 access-list**
- **policy static** or **nat** commands
- **ssh**
- **telnet**

If you are in manual-commit mode and you need to change one of the previously listed commands, change the mode to **manual-commit** and commit the changes before they take effect.

While you are in manual-commit mode, do not enter a command that binds a configuration for a previouly listed command that has been added to but not committed to an interface. For example, if an **access-list 'foo'** command has been added in manual-commit mode and that change has not been committed, do not enter the **access-group** command that binds **foo** to an interface. Commit **foo** first through the **access-list commit** command and only then enter the **access-group** command.

In manual-commit mode, deleting an ACE flags it for deletion and also removes it from the running configuration. When you enter the **show running** command before you enter the **access-list commit** command, the original configuration with the following qualifier text “uncommitted deletion” displays. Adding an ACE flags it as added but not as committed. When you enter the **show running** command before you enter the **access-list commit** command, the original configuration with the following qualifier text “uncommitted addition” displays. When the **access-list commit** command runs, these qualifiers are removed and the configurations become active.

Examples

This example shows how to flag and add the access-list rules:

```
fwsm/context(config)# access-list commit
```

Related Commands

access-group
access-list extended
access-list mode
clear access-list
object-group
show access-list

access-list deny-flow-max

To specify the maximum number of concurrent deny flows that can be created, use the **access-list deny-flow-max** command. To return to the default settings, use the **no** form of this command.

[**no**] **access-list deny-flow-max** *n*

Syntax Description

n	Maximum number of concurrent ACL deny flows that can be created; valid values are from 1 to 4096.

Defaults

The default is 4096.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Syslog message 106101 is generated when the FWSM has reached the maximum number, *n*, of ACL deny flows.

Examples

This example shows how to specify the maximum number of concurrent deny flows that can be created:

```
fwsm/context(config)# access-list deny-flow-max 256
```

Related Commands

access-list extended
clear access-list
show access-list

access-list ethertype

To add an EtherType access list to the configuration and to configure policy for IP traffic through the firewall, use the **access-list ethertype** command. To remove the access list, use the **no** form of this command.

[**no**] **access-list** *id* **ethertype** {**deny** | **permit**} *ether-value* [**unicast** | **multicast** | **broadcast**]

Syntax Description

id	Name or number of an access list.
deny	Denies access if the conditions are matched. See the "Usage Guidelines" section for the description.
permit	Permits access if the conditions are matched. See the "Usage Guidelines" section for the description.
ether-value	Ethernet value.
unicast	(Optional) Specifies unicast notification.
multicast	(Optional) Specifies multicast notification.
broadcast	(Optional) Specifies broadcast notification.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for denied packets—Deny packets must be present to log denied packets.
- When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to add an EtherType access list:

```
fwsm/context(config)# access-list my_access ethertype permit unicast
```

Related Commands

access-group
access-list commit
access-list extended
access-list mode
clear access-group
clear access-list
configure
object-group
pager
show access-group
show access-list

access-list extended

To add an access list to the configuration and to configure policy for IP traffic through the firewall, use the **access-list extended** command. To remove the access list, use the **no** form of this command.

[**no**] **access-list** *id* **extended deny** | **permit** *protocol* | **object-group** *protocol_obj_grp_id* **host** *source_ip* | *source_mask* | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*] *destination_ip destination_mask* | **object-group** *network_obj_grp_id* [*operator port* [*port*] | **object-group** *service_obj_grp_id*]} [**log** [**disable**] | [*level*] | [**default**] | [**interval** *secs*]]

Syntax Description

id	Name or number of an access list.
extended	Specifies an extended access list.
deny	Denies access if the conditions are matched. See the "Usage Guidelines" section for the description.
permit	Permits access if the conditions are matched. See the "Usage Guidelines" section for the description.
protocol	Name or number of an IP protocol; valid values are **icmp**, **ip**, **tcp**, or **udp**, or an integer in the range 1 to 254 representing an IP protocol number. See the "Usage Guidelines" section for additional information.
object-group	Specifies an object group; see the "Usage Guidelines" section for additional information.
protocol_obj_grp_id	Existing protocol object group identification.
source_ip	Address of the network or host local to the FWSM; see the "Usage Guidelines" section for additional information.
source_mask	Netmask bits (mask) to be applied to the *source_addr* if the source address is for a network mask.
network_obj_grp_id	Existing network object group identification.
operator	Operand that will compare the source IP address to the destination IP address; see the "Usage Guidelines" section for additional information.
port	(Optional) Port that you permit or deny services access; see the "Usage Guidelines" section for additional information.
service_obj_grp_id	(Optional) Object group.
destination_ip	IP address of the network or host to which the packet is being sent; see the "Usage Guidelines" section for additional information.
destination_mask	Netmask bits (mask) to be applied to *destination_addr* if the destination address is a network mask.
log default	(Optional) Specifies that a syslog message 106100 is generated for the ACE. See the "Usage Guidelines" section for information.
log disable	(Optional) Disables syslog messaging. See the "Usage Guidelines" section for information.
log *level*	(Optional) Specifies the syslog level; valid values are from 0 to 7. See the "Usage Guidelines" section for information.
interval *secs*	(Optional) Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for only specified deny packets—Deny packets must be present to log denied packets.
- When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When used with the **access-group** command, the **deny** optional keyword does not allow a packet to traverse the FWSM. By default, the FWSM denies all packets on the originating interface unless you specifically permit access.

When you specify the *protocol* to match any Internet protocol, including TCP and UDP, use the **ip** keyword.

Refer to the **object-group** command for information on how to configure object groups.

The *operator* compares the source IP address (*sip*) or destination IP address (*dip*) ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **access-list** command without an operator and port to indicate all ports by default as follows:

```
fwsm/context(config)# access-list acl_out permit tcp any host 209.165.201.1
```

Use **eq** and a port to permit or deny access to just that port. For example, use **eq ftp** to permit or deny access only to FTP:

```
fwsm/context(config)# access-list acl_out deny tcp any host 209.165.201.1 eq ftp
```

Use **lt** and a port to permit or deny access to all ports less than the port that you specify. For example, use **lt 2025** to permit or deny access to the well-known ports (1 to 1024):

```
fwsm/context(config)# access-list acl_dmz1 permit tcp any host 192.168.1.1 lt 1025
```

Use **gt** and a port to permit or deny access to all ports greater than the port that you specify. For example, use **gt 42** to permit or deny ports 43 to 65535:

```
fwsm/context(config)# access-list acl_dmz1 deny udp any host 192.168.1.2 gt 42
```

Use **neq** and a port to permit or deny access to every port except the ports that you specify. For example, use **neq 10** to permit or deny ports 1–9 and 11 to 65535:

```
fwsm/context(config)# access-list acl_dmz1 deny tcp any host 192.168.1.3 neq 10
```

Use **range** and a port range to permit or deny access to only those ports named in the range. For example, use **range 10 1024** to permit or deny access only to ports 10 through 1024. All other ports are unaffected. The use of port ranges can dramatically increase the number of IPSec tunnels. For example, if a port range of 5000 to 65535 is specified for a highly dynamic protocol, up to 60,535 tunnels can be created.

Enter *port* to specify services by the port that handles it, such as **smtp for port 25**, **www** for port 80, and so on. You can specify ports by either a literal name or a number in the range of 0 to 65535. Refer to valid port numbers at this URL:

http://www.iana.org/assignments/port-numbers

See the "Specifying Port Values" section in Appendix B for a list of valid port literal names in port ranges. You can also specify numbers.

For the **log disable | default |** *level* optional keyword, use these guidelines:

- When you specify the **log** optional keyword, it generates syslog message 106100 for the ACE to which it is applied. (syslog message 106100 is generated for every matching permit or deny ACE flow passing through the FWSM.) The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show access-list** command for the ACE, and new 106100 messages are generated at the end of the interval that is defined by **interval** *secs* if the hit count for the flow is not zero.
- The default ACL logging behavior (the **log** keyword is not specified) is that if a packet is denied, then message 106023 is generated. If a packet is permitted, then no syslog message is generated.
- You can specify an optional syslog *level* (0–7) for the generated syslog messages (106100). If no *level* is specified, the default level is 6 (informational) for a new ACE. If the ACE already exists, then its existing log level remains unchanged.
- If you do not specify the **log disable** optional keyword, the access list logging is completely disabled. No syslog message, including message 106023, is generated.
- The **log default** optional keyword restores the default access list logging behavior.

Note Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for additional information about logging.

The **interval** *secs* keyword and argument are used as the timeout value for deleting an inactive flow. If you do not specify the **interval** *secs* optional keyword, the default interval is 300 seconds for a new ACE. If an ACE already exists, any interval that was previously associated with that ACE remains unchanged.

The *icmp_type* argument is for non-IPSec use only or for permit or deny access to ICMP message types (see Table 2-1 on page 2-44). You should omit this optional keyword to indicate all ICMP types.

ICMP message types are not supported with IPSec. When the **access-list** command is used with the **crypto map** command, the *icmp_type* is ignored.

The **access-list** command allows you to specify if an IP address is permitted or denied access to a port or protocol. One or more **access-list** commands with the same access list name are referred to as an "access list." Access lists that are associated with IPSec are known as "crypto access lists."

You can use the **object-group** command to group access lists.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. We do not recommend that you use this keyword with IPSec.
- Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Use the following guidelines for specifying a network mask:

- Do not specify a mask if the address is for a host; if the destination address is for a host, use the **host** keyword before the address as follows:

```
fwsm/context(config)# access-list acl_grp permit tcp any host 192.168.1.1
```

- If the address is a network address, specify the mask as a 32-bit quantity in four-part, dotted-decimal format. Place zeros in the bit positions that you want to ignore.
- Remember that you specify a network mask differently than with the Cisco IOS software **access-list** command. With the FWSM, enter **255.0.0.0** for a Class A address, **255.255.0.0** for a Class B address, and **255.255.255**.0 for a Class C address. If you are using a subnetted network address, use the appropriate network mask as follows:

```
fwsm/context(config)# access-list acl_grp permit tcp any 209.165.201.0 255.255.255.224
```

The **access-list** command supports the **sunrpc** service.

The **show access-list** command lists the **access-list** commands in the configuration and the hit count of the number of times each element has been matched during an **access-list** command search. Additionally, it displays the number of access list statements in the access list and indicates whether or not the list is configured for Turbo ACL. If the list has fewer than 18 ACEs, it is marked as turbo-configured but is not actually configured for Turbo ACL until there are 19 or more entries.

The **show access-list** *source_addr* optional keyword and argument filter the show output so that only those access-list elements that match the source IP address (or with **any** as source IP address) are displayed.

The **clear access-list** command removes all **access-list** commands from the configuration or, if specified, removes the access lists by their *id*. The **clear access-list** *id* **counters** command clears the hit count for the specified access list.

The **no access-list** command removes an **access-list** command from the configuration. If you remove all the **access-list** commands in an access list, the **no access-list** command also removes the corresponding **access-group** command from the configuration.

Note The **aaa**, **crypto map**, and **icmp** commands use the **access-list** commands.

access-list logging Commands

This example shows what happens when you enable an **access-list log** optional keyword:

```
fwsm/context(config)# access-group outside-acl in interface outside
fwsm/context(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval
600
fwsm/context(config)# access-list outside-acl permit ip host 2.2.2.2 any
fwsm/context(config)# access-list outside-acl deny ip any any log 2
```

The previous example shows the use of access-list logging in an ICMP context:

1. An ICMP echo request (1.1.1.1 -> 192.168.1.1) arrives on the outside interface.
2. An ACL called **outside-acl** is applied for the access check.
3. The packet is permitted by the first ACE of **outside-acl** that has the **log** optional keyword enabled.
4. The log flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) has not been cached, so the following syslog message is generated and the log flow is cached:

```
106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
inside/192.168.1.1(8) hit-cnt 1 (first hit)
```

5. Twenty packets arrive on the outside interface within the next 10 minutes (600 seconds). Because the log flow has been cached, the log flow is located and the hit count of the log flow is incremented for each packet.
6. At the end of 10 minutes, this syslog message is generated and the hit count of the log flow is reset to 0:

```
106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
inside/192.168.1.1(8) hit-cnt 20 (300-second interval)
```

7. No packets arrive on the outside interface within the next 10 minutes, so the hit count of the log flow remains 0.
8. At the end of 20 minutes, the cached flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) is deleted because of the 0 hit count.

To disable a **log** optional keyword without removing the ACE, enter the **access-list** *id* **log disable** command.

When removing an ACE with a **log** optional keyword enabled using the **no access-list** command, you do not need to specify all the **log** options. The ACE is removed if its permit or deny rule is used to uniquely identify it. However, removing an ACE (with a **log** optional keyword enabled) does not remove the associated cached flows. You must remove the entire ACL to remove the cached flows. When a cached flow is flushed due to the removal of an ACL, a syslog message is generated if the hit count of the flow is nonzero.

Use the **clear access-list** command to remove all the cached flows.

access-list *id* remark command

You can access the **access-list** *id* [**line** *line-num*] **remark** *text* command to include comments (remarks) about entries in any ACL. You can use remarks to make the ACL easier to scan and interpret. Each remark line is limited to 100 characters.

The ACL remark can go before or after an **access-list** command, but you should place it in a consistent position so that it is clear which remark describes which **access-list** command.

The **no access-list** *id* **line** *line-num* **remark** *text* and **no access-list** *id* **line** *line-num* commands both remove the remark at that line number.

The following are samples of possible access-list remarks:

```
access-list out-acl remark - ACL for the outside interface
access-list out-acl remark - Allow Joe Smith's group to login
access-list out-acl permit tcp 1.1.1.0 255.255.255.0 server
access-list out-acl remark - Allow Lee White's group to login
access-list out-acl permit tcp 1.1.3.0 255.255.255.0 server
access-list out-acl remark - Deny known hackers
access-list out-acl deny ip host 192.23.56.1 any
access-list out-acl deny ip host 197.1.1.125 any
```

RADIUS Authorization

The FWSM allows a RADIUS server to send user group attributes to the FWSM in the RADIUS authentication response message. Additionally, the FWSM allows downloadable access lists from the RADIUS server. For example, you can configure an access list on a Cisco Secure ACS server and download it to the FWSM during RADIUS authorization.

After the FWSM authenticates a user, it can use the CiscoSecure **acl** attribute that is returned by the authentication server to identify an access list for a given user group. The firewall also provides the same functionality for TACACS+.

To restrict users to three servers and deny everything else, the **access-list** commands are as follows:

```
fwsm/context(config)# access-list eng permit ip any server1 255.255.255.255
fwsm/context(config)# access-list eng permit ip any server2 255.255.255.255
fwsm/context(config)# access-list eng permit ip any server3 255.255.255.255
fwsm/context(config)# access-list eng deny ip any any
```

In this example, the vendor-specific attribute string in the CiscoSecure configuration is set to **acl=eng**. This field in the CiscoSecure configuration contains the **access-list** identification name. The FWSM gets the **acl=***id* from CiscoSecure and extracts the ACL number from the attribute string, which it places in a user's uauth entry. When a user tries to open a connection, the FWSM checks the access list in the user's uauth entry, and depending on the permit or deny status of the access list match, permits or denies the connection. When a connection is denied, the FWSM generates a syslog message. If there is no match, then the implicit rule is to deny.

Because the source IP of a given user can vary depending on where the user is logging in from, you should set the source address in the **access-list** command to **any** and the destination address to identify which network services to which the user is permitted or denied access. To specify that only the users logging in from a given subnet can use the specified services, you should specify the subnet instead of using **any**.

Note An access list that is used for RADIUS authorization does not require an **access-group** command to bind the statements to an interface.

The **aaa authorization** command does not have a **radius** optional keyword.

Configure the access list that is listed in Attribute 11 to specify a per-user access list name. Otherwise, remove Attribute 11 from the configuration if no access list is intended for user authentication. If the access list is not configured on the FWSM when the user attempts to login, the login will fail.

For more information, refer to the *Cisco FWSM and VPN Configuration Guide*.

Usage Notes

The **clear access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** commands referencing the access list are incomplete. To correct the condition, either define other **access-list** commands to complete the **crypto map** commands or remove the **crypto map** commands that pertain to the **access-list** command. Refer to the **crypto map client** command for more information.

ACLs that are dynamically updated on the FWSM by an AAA server can only be shown using the **show access-list** command. The **write** command does not save or display these updated lists.

The **access-list** command operates on a first-match basis.

If you specify an **access-list** command and bind it to an interface with the **access-group** command, by default, all traffic to that interface is denied. You must explicitly permit traffic. Inbound refers to traffic passing through the interface, not the traffic passing from a lower security level interface to a higher security level interface.

Always permit access first and then deny access afterward. If the host entries match, use the **permit** keyword; otherwise, use the default **deny** keyword. You only need to specify additional **deny** keywords if you need to deny specific hosts and permit everyone else.

You can see the security levels for interfaces with the **show nameif** command.

The optional ICMP message type (*icmp_type*) argument is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.

You can bind only one access list to an interface using the **access-group** command.

If you specify the **permit** optional keyword in the access list, the FWSM continues to process the packet. If you specify the **deny** optional keyword in the access list, the FWSM discards the packet and generates this syslog message:

```
%fwsm#-4-106019: IP packet from source_addr to destination_addr, protocol protocol
received from interface interface_name deny by access-group id
```

The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command *except* that the FWSM uses a subnet mask. (Cisco IOS software uses a wildcard mask.) For example, in the Cisco IOS software **access-list** command, a subnet mask of 0.0.0.255 would be specified as 255.255.255.0 in the FWSM **access-list** command.

We recommend that you do not use the **access-list** command with the **outbound** command. Using these commands together may cause debugging issues. The **outbound** command operates from one interface to another and the **access-list** command when used with the **access-group** command applies only to a single interface. If you use these commands together, the FWSM evaluates the **access-list** command before checking the **outbound** command.

Refer to Chapter 3, "Managing Network Access and Use" in the *Cisco Firewall and VPN Configuration Guide* for a detailed description about using the **access-list** command to provide server access and to restrict outbound user access.

See the **aaa-server radius-acctport** and **aaa-server radius-authport** commands to verify or change port settings.

ICMP Message Types

For non-IPSec use only, if you prefer more selective ICMP access, you can specify a single ICMP message type as the last optional keyword in this command. Table 2-1 lists the possible ICMP types values.

Table 2-1 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	address-mask-request

Table 2-1 ICMP Type Literals (continued)

ICMP Type	Literal
18	address-mask-reply
31	conversion-error
32	mobile-redirect

This example shows that if you specify an ICMP message type for use with IPSec, FWSM ignores it:

```
fwsm/context(config)# access-list 10 permit icmp any any echo-reply
```

IPSec is enabled so that a **crypto map** command references the *id* for this **access-list** command, and then the **echo-reply** ICMP message type is ignored.

Using the access-list Command with IPSec

If you bind an access list to an interface with the **access-group** command, the access list selects which traffic can traverse the FWSM. When bound to a **crypto map** command, the access list selects which IP traffic IPSec protects and which traffic IPSec does not protect. For example, access lists can be created to protect all IP traffic between Subnet X and Subnet Y or traffic between Host A and Host B.

The access lists are not specific to IPSec. The **crypto map** command referring to the specific access list defines whether IPSec processing is applied to the traffic matching a permit in the access list.

Crypto access lists that are associated with the IPSec **crypto map** command have these primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
- Process traffic to filter out and discard traffic that IPSec protects.
- Determine whether to accept requests for IPSec security associations for the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is only done for the **crypto map** commands with the **ipsec-isakmp** optional keyword.) A peer's initiated IPSec negotiation will be accepted only if you specify a data flow that is permitted by a crypto access list that is associated with an **ipsec-isakmp** crypto map entry.

You can associate a crypto access list with an interface by defining the corresponding **crypto map** command and applying the crypto map set to an interface. You must use different access lists in different entries of the same crypto map set. The access list's criteria are applied in the forward direction to traffic exiting your FWSM and the reverse direction to traffic entering your FWSM.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries that specify different IPSec policies.

We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword.

If you configure multiple entries for a given crypto access list, the first **permit** keyword entry matched will be the entry used to determine the scope of the IPSec security association. The IPSec security association will be set up to protect traffic that meets the criteria of the matched keyword entry only. If traffic matches a different **permit** entry of the crypto access list, a new, separate IPSec security association will be negotiated to protect traffic matching the newly matched **access list** command.

Some services, such as FTP, require two **access-list** commands, one for port 10 and another for port 21, to properly encrypt FTP traffic.

Examples

This example shows how to create a numbered access list that specifies a Class C subnet for the source and a Class C subnet for the destination of IP packets. Because the **access-list** command is referenced in the **crypto map** command, the FWSM encrypts all IP traffic that is exchanged between the source and destination subnets.

```
fwsm/context(config)# access-list 101 permit ip 172.21.3.0 255.255.0.0 172.22.2.0
255.255.0.0
fwsm/context(config)# access-group 101 in interface outside
fwsm/context(config)# crypto map mymap 10 match address 101
```

This example shows how to let only an ICMP message type of echo-reply be permitted into the outside interface:

```
fwsm/context(config)# access-list acl_out permit icmp any any echo-reply
fwsm/context(config)# access-group acl_out interface outside
```

This example shows how ACEs are numbered by the FWSM and how remarks are inserted (remarks are not assigned a line number):

```
fwsm/context(config)# show access-list ac
access-list ac; 2 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)

fwsm/context(config)# access-list ac permit tcp object-group remote object-group locals
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac line 3 permit tcp object-group remote object-group locals
fwsm/context(config)# access-list ac remark This comment describes the ACE line 3

fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp object-group remote object-group locals

fwsm/context(config)# access-list ac permit tcp 171.0.0.0 255.0.0.0 any
fwsm/context(config)# show access-list ac
access-list ac; 4 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp object-group remote object-group locals
access-list ac line 4 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)

fwsm/context(config)# no access-list ac permit tcp object-group remote object-group locals
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
```

```
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)
```

This example shows how to remove an access list comment:

```
fwsm/context(config)# access-list ac remark This comment diatribes the ACE line 5
fwsm/context(config)# sh access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)
access-list ac remark This comment describes the ACE line 5

fwsm/context(config)# no access-list ac remark This comment describes the ACE line 5
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac permit ip any any line 1 (hitcnt=0)
access-list ac permit tcp any any line 2 (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac permit tcp 171.0.0.0 255.0.0.0 any line 4 (hitcnt=0)
```

This example shows how to insert an access list entry at a specific line number:

```
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)

fwsm/context(config)# access-list ac line 3 permit ip 172.0.0.0 255.0.0.0 any
fwsm/context(config)# show access-list ac
access-list ac; 4 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit ip 172.0.0.0 255.0.0.0 any (hitcnt=0)
access-list ac line 4 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)
```

The **show access-list** command has the following line of output which shows the total number of cached ACL log flows (total), the number of cached deny-flows (denied), and the maximum number of allowed deny-flows:

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
```

Related Commands

access-group
access-list commit
access-list extended
access-list mode
clear access-group
clear access-list
configure
object-group
pager
show access-group
show access-list

access-list icmp host

To add an ICMP host access list to the configuration and to configure policy for IP traffic through the FWSM, use the **access-list icmp host** command. To remove the access list, use the **no** form of this command.

[**no**] **access-list** *id* {**deny** | **permit**} **host** {*source_ip* | {*source_ip source_mask*}} [**log** [**disable** | [*level*] | **default**] | [**interval** *secs*]]

Syntax Description

id	Name or number of an access list.
deny	Denies access if the conditions are matched. See the "Usage Guidelines" section for the description.
permit	Permits access if the conditions are matched. See the "Usage Guidelines" section for the description.
host	Specifies that you are adding a host to the access list.
source_ip	IP address of the network or host from which the packet is being sent.
source_mask	Netmask bits (mask) to be applied to the *source_addr* if the source address is for a network mask.
log disable	(Optional) Disables syslog messaging. See the "Usage Guidelines" section for information.
log default	(Optional) Specifies that a syslog message 106100 is generated for ACE. See the "Usage Guidelines" section for information.
log *level*	(Optional) Specifies the syslog level; valid values are from 0 to 7. See the "Usage Guidelines" section for information.
interval *secs*	(Optional) Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for denied packets—Deny packets must be present to log denied packets.
- When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When used with the **access-group** command, the **deny** optional keyword does not allow a packet to traverse the FWSM. By default, the FWSM denies all packets on the originating interface unless you specifically permit access.

For the **log disable | default |** *level* optional keyword, use these guidelines:

- When you specify the **log** optional keyword, it generates syslog message 106100 for the ACE to which it is applied. (syslog message 106100 is generated for every matching permit or deny ACE flow passing through the FWSM.) The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show access-list** command for the ACE, and new 106100 messages are generated at the end of the interval that is defined by **interval** *secs* if the hit count for the flow is not zero.
- The default ACL logging behavior (the **log** keyword is not specified) is that if a packet is denied, then message 106023 is generated. If a packet is permitted, then no syslog message is generated.
- You can specify an optional syslog *level* (0–7) for the generated syslog messages (106100). If no *level* is specified, the default level is 6 (informational) for a new ACE. If the ACE already exists, then its existing log level remains unchanged.
- If you do not specify the **log disable** optional keyword, the access list logging is completely disabled. No syslog message, including message 106023, is generated.
- The **log default** optional keyword restores the default access list logging behavior.

Note Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for additional information about logging.

The **access-list** command allows you to specify if an IP address is permitted or denied access to a port or protocol. One or more **access-list** commands with the same access list name are referred to as an "access list." Access lists that are associated with IPSec are known as "crypto access lists."

You can use the **object-group** command to group access lists.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. We do not recommend that you use this keyword with IPSec.
- Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Use the following guidelines for specifying a network mask:

- Do not specify a mask if the address is for a host; if the destination address is for a host, use the **host** keyword before the address as follows:

```
fwsm/context(config)# access-list acl_grp permit tcp any host 192.168.1.1
```

- If the address is a network address, specify the mask as a 32-bit quantity in four-part, dotted-decimal format. Place zeros in the bit positions that you want to ignore.
- Remember that you specify a network mask differently than with the Cisco IOS software **access-list** command. With the FWSM, enter **255.0.0.0** for a Class A address, **255.255.0.0** for a Class B address, and **255.255.255**.0 for a Class C address. If you are using a subnetted network address, use the appropriate network mask as follows:

```
fwsm/context(config)# access-list acl_grp permit tcp any 209.165.201.0 255.255.255.224
```

The **access-list** command supports the **sunrpc** service.

The **show access-list** command lists the **access-list** commands in the configuration and the hit count of the number of times each element has been matched during an **access-list** command search. Additionally, it displays the number of access list statements in the access list and indicates whether or not the list is configured for Turbo ACL. If the list has fewer than 18 ACEs, it is marked as turbo-configured but is not actually configured for Turbo ACL until there are 19 or more entries.

The **show access-list** *source_addr* optional keyword and argument filter the show output so that only those access-list elements that match the source IP address (or with **any** as source IP address) are displayed.

The **clear access-list** command removes all **access-list** commands from the configuration or, if specified, access lists by their *id*. The **clear access-list** *id* **counters** command clears the hit count for the specified access list.

The **no access-list** command removes an **access-list** command from the configuration. If you remove all the **access-list** commands in an access list, the **no access-list** command also removes the corresponding **access-group** command from the configuration.

Note The **aaa**, **crypto map**, and **icmp** commands use the **access-list** commands.

access-list logging Commands

This example shows what happens when you enable an **access-list log** optional keyword:

```
fwsm/context(config)# access-group outside-acl in interface outside
fwsm/context(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7 interval
600
fwsm/context(config)# access-list outside-acl permit ip host 2.2.2.2 any
fwsm/context(config)# access-list outside-acl deny ip any any log 2
```

The previous example shows the use of access-list logging in an ICMP context:

1. An ICMP echo request (1.1.1.1 -> 192.168.1.1) arrives on the outside interface.
2. An ACL called **outside-acl** is applied for the access check.
3. The packet is permitted by the first ACE of **outside-acl** that has the **log** optional keyword enabled.
4. The log flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) has not been cached, so the following syslog message is generated and the log flow is cached:

   ```
   106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
   inside/192.168.1.1(8) hit-cnt 1 (first hit)
   ```

5. Twenty packets arrive on the outside interface within the next 10 minutes (600 seconds). Because the log flow has been cached, the log flow is located and the hit count of the log flow is incremented for each packet.
6. At the end of 10 minutes, this syslog message is generated and the hit count of the log flow is reset to 0:

   ```
   106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
   inside/192.168.1.1(8) hit-cnt 20 (300-second interval)
   ```

7. No packets arrive on the outside interface within the next 10 minutes, so the hit count of the log flow remains 0.
8. At the end of 20 minutes, the cached flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) is deleted because of the 0 hit count.

To disable a **log** optional keyword without removing the ACE, enter the **access-list** *id* **log disable** command.

When removing an ACE with a **log** optional keyword enabled using the **no access-list** command, you do not need to specify all the log options. The ACE is removed if its permit or deny rule is used to uniquely identify it. However, removing an ACE (with a **log** optional keyword enabled) does not remove the associated cached flows. You must remove the entire ACL to remove the cached flows. When a cached flow is flushed due to the removal of an ACL, a syslog message is generated if the hit count of the flow is nonzero.

Use the **clear access-list** command to remove all the cached flows.

access-list *id* remark command

You can access the **access-list** *id* [**line** *line-num*] **remark** *text* command to include comments (remarks) about entries in any ACL. You can use remarks to make the ACL easier to scan and interpret. Each remark line is limited to 100 characters.

The ACL remark can go before or after an **access-list** command, but you should place it in a consistent position so that it is clear which remark describes which **access-list** command.

The **no access-list** *id* **line** *line-num* **remark** *text* and **no access-list** *id* **line** *line-num* commands both remove the remark at that line number.

The following are samples of possible access-list remarks:

```
access-list out-acl remark - ACL for the outside interface
access-list out-acl remark - Allow Joe Smith's group to login
access-list out-acl permit tcp 1.1.1.0 255.255.255.0 server
access-list out-acl remark - Allow Lee White's group to login
access-list out-acl permit tcp 1.1.3.0 255.255.255.0 server
access-list out-acl remark - Deny known hackers
access-list out-acl deny ip host 192.23.56.1 any
access-list out-acl deny ip host 197.1.1.125 any
```

RADIUS Authorization

The FWSM allows a RADIUS server to send user group attributes to the FWSM in the RADIUS authentication response message. Additionally, the FWSM allows downloadable access lists from the RADIUS server. For example, you can configure an access list on a Cisco Secure ACS server and download it to the FWSM during RADIUS authorization.

After the FWSM authenticates a user, it can use the CiscoSecure **acl** attribute that is returned by the authentication server to identify an access list for a given user group. The firewall also provides the same functionality for TACACS+.

To restrict users to three servers and deny everything else, the **access-list** commands are as follows:

```
fwsm/context(config)# access-list eng permit ip any server1 255.255.255.255
fwsm/context(config)# access-list eng permit ip any server2 255.255.255.255
fwsm/context(config)# access-list eng permit ip any server3 255.255.255.255
fwsm/context(config)# access-list eng deny ip any any
```

In this example, the vendor-specific attribute string in the CiscoSecure configuration is set to **acl=eng**. This field in the CiscoSecure configuration contains the **access-list** identification name. The FWSM gets the **acl=***id* from CiscoSecure and extracts the ACL number from the attribute string, which it places in a user's uauth entry. When a user tries to open a connection, the FWSM checks the access list in the user's uauth entry, and depending on the permit or deny status of the access list match, permits or denies the connection. When a connection is denied, the FWSM generates a syslog message. If there is no match, then the implicit rule is to deny.

Because the source IP of a given user can vary depending on where the user is logging in from, you should set the source address in the **access-list** command to **any** and the destination address to identify which network services to which the user is permitted or denied access. To specify that only the users logging in from a given subnet can use the specified services, you should specify the subnet instead of using **any**.

Note An access list that is used for RADIUS authorization does not require an **access-group** command to bind the statements to an interface.

The **aaa authorization** command does not have a **radius** optional keyword.

Configure the access list that is listed in Attribute 11 to specify a per-user access list name. Otherwise, remove Attribute 11 from the configuration if no access list is intended for user authentication. If the access list is not configured on the FWSM when the user attempts to login, the login will fail.

For more information, refer to the *Cisco FWSM and VPN Configuration Guide*.

Usage Notes

The **clear access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** commands referencing the access list are incomplete. To correct the condition, either define other **access-list** commands to complete the **crypto map** commands or remove the **crypto map** commands that pertain to the **access-list** command. Refer to the **crypto map client** command for more information.

ACLs that are dynamically updated on the FWSM by an AAA server can only be shown using the **show access-list** command. The **write** command does not save or display these updated lists.

The **access-list** command operates on a first-match basis.

If you specify an **access-list** command and bind it to an interface with the **access-group** command, by default, all traffic to that interface is denied. You must explicitly permit traffic. Inbound refers to traffic passing through the interface, not the traffic passing from a lower security level interface to a higher security level interface.

Always permit access first and then deny access afterward. If the host entries match, use the **permit** keyword; otherwise, use the default **deny** keyword. You only need to specify additional **deny** keywords if you need to deny specific hosts and permit everyone else.

You can see the security levels for interfaces with the **show nameif** command.

The ICMP message type (*icmp_type*) optional argument is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.

You can bind only one access list to an interface using the **access-group** command.

If you specify the **permit** optional keyword in the access list, the FWSM continues to process the packet. If you specify the **deny** optional keyword in the access list, the FWSM discards the packet and generates this syslog message:

```
%fwsm#-4-106019: IP packet from source_addr to destination_addr, protocol protocol
received from interface interface_name deny by access-group id
```

The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command *except* that the FWSM uses a subnet mask. (Cisco IOS software uses a wildcard mask.) For example, in the Cisco IOS software **access-list** command, a subnet mask of 0.0.0.255 would be specified as 255.255.255.0 in the FWSM **access-list** command.

We recommend that you do not use the **access-list** command with the **outbound** command. Using these commands together may cause debugging issues. The **outbound** command operates from one interface to another and the **access-list** command when used with the **access-group** command applies only to a single interface. If you use these commands together, the FWSM evaluates the **access-list** command before checking the **outbound** command.

Refer to Chapter 3, "Managing Network Access and Use" in the *Cisco Firewall and VPN Configuration Guide* for a detailed description about using the **access-list** command to provide server access and to restrict outbound user access.

See the **aaa-server radius-acctport** and **aaa-server radius-authport** commands to verify or change port settings.

ICMP Message Types

For non-IPSec use only, if you prefer more selective ICMP access, you can specify a single ICMP message type as the last optional keyword in this command. Table 2-2 lists the possible ICMP types values.

Table 2-2 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	address-mask-request
18	address-mask-reply
31	conversion-error
32	mobile-redirect

This example shows that if you specify an ICMP message type for use with IPSec, FWSM ignores it:

```
fwsm/context(config)# access-list 10 permit icmp any any echo-reply
```

IPSec is enabled so that a **crypto map** command references the *id* for this **access-list** command, and then the **echo-reply** ICMP message type is ignored.

Using the access-list Command with IPSec

If you bind an access list to an interface with the **access-group** command, the access list selects which traffic can traverse the FWSM. When bound to a **crypto map** command, the access list selects which IP traffic IPSec protects and which traffic IPSec does not protect. For example, access lists can be created to protect all IP traffic between Subnet X and Subnet Y or traffic between Host A and Host B.

The access lists are not specific to IPSec. The **crypto map** command referring to the specific access list defines whether IPSec processing is applied to the traffic matching a permit in the access list.

Crypto access lists that are associated with the IPSec **crypto map** command have these primary functions:

- Select outbound traffic to be protected by IPSec (permit = protect).
- Indicate the data flow to be protected by the new security associations (specified by a single permit entry) when initiating negotiations for IPSec security associations.
- Process traffic to filter out and discard traffic that IPSec protects.
- Determine whether to accept requests for IPSec security associations for the requested data flows when processing IKE negotiation from the IPSec peer. (Negotiation is only done for the **crypto map** commands with the **ipsec-isakmp** optional keyword.) A peer's initiated IPSec negotiation will be accepted only if you specify a data flow that is permitted by a crypto access list that is associated with an **ipsec-isakmp** crypto map entry.

You can associate a crypto access list with an interface by defining the corresponding **crypto map** command and applying the crypto map set to an interface. You must use different access lists in different entries of the same crypto map set. The access list's criteria are applied in the forward direction to traffic exiting your FWSM and the reverse direction to traffic entering your FWSM.

If you want certain traffic to receive one combination of IPSec protection (for example, authentication only) and other traffic to receive a different combination of IPSec protection (for example, both authentication and encryption), you need to create two different crypto access lists to define the two different types of traffic. These different access lists are then used in different crypto map entries that specify different IPSec policies.

We recommend that you configure "mirror image" crypto access lists for use by IPSec and that you avoid using the **any** keyword.

If you configure multiple entries for a given crypto access list, the first **permit** keyword entry matched will be the entry used to determine the scope of the IPSec security association. The IPSec security association will be set up to protect traffic that meets the criteria of the matched keyword entry only. Later, if traffic matches a different **permit** entry of the crypto access list, a new, separate IPSec security association will be negotiated to protect traffic matching the newly matched **access list** command.

Some services, such as FTP, require two **access-list** commands, one for port 10 and another for port 21, to properly encrypt FTP traffic.

Examples

This example shows how to create a numbered access list that specifies a Class C subnet for the source and a Class C subnet for the destination of IP packets. Because the **access-list** command is referenced in the **crypto map** command, the FWSM encrypts all IP traffic that is exchanged between the source and destination subnets.

```
fwsm/context(config)# access-list 101 permit ip 172.21.3.0 255.255.0.0 172.22.2.0
255.255.0.0
fwsm/context(config)# access-group 101 in interface outside
fwsm/context(config)# crypto map mymap 10 match address 101
```

This example shows how to let only an ICMP message type of echo-reply be permitted into the outside interface:

```
fwsm/context(config)# access-list acl_out permit icmp any any echo-reply
fwsm/context(config)# access-group acl_out interface outside
```

This example shows how ACEs are numbered by the FWSM and how remarks are inserted (remarks are not assigned a line number):

```
fwsm/context(config)# show access-list ac
access-list ac; 2 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)

fwsm/context(config)# access-list ac permit tcp object-group remote object-group locals
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac line 3 permit tcp object-group remote object-group locals
fwsm/context(config)# access-list ac remark This comment describes the ACE line 3

fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp object-group remote object-group locals

fwsm/context(config)# access-list ac permit tcp 171.0.0.0 255.0.0.0 any
fwsm/context(config)# show access-list ac
access-list ac; 4 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp object-group remote object-group locals
access-list ac line 4 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)

fwsm/context(config)# no access-list ac permit tcp object-group remote object-group locals
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)
```

This example shows how to remove an access list comment:

```
fwsm/context(config)# access-list ac remark This comment diatribes the ACE line 5
fwsm/context(config)# sh access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)
access-list ac remark This comment describes the ACE line 5

fwsm/context(config)# no access-list ac remark This comment describes the ACE line 5
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac permit ip any any line 1 (hitcnt=0)
access-list ac permit tcp any any line 2 (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac permit tcp 171.0.0.0 255.0.0.0 any line 4 (hitcnt=0)
```

This example shows how to insert an access list entry at a specific line number:

```
fwsm/context(config)# show access-list ac
access-list ac; 3 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)

fwsm/context(config)# access-list ac line 3 permit ip 172.0.0.0 255.0.0.0 any
fwsm/context(config)# show access-list ac
access-list ac; 4 elements
access-list ac line 1 permit ip any any (hitcnt=0)
access-list ac line 2 permit tcp any any (hitcnt=0)
access-list ac remark This comment describes the ACE line 3
access-list ac line 3 permit ip 172.0.0.0 255.0.0.0 any (hitcnt=0)
access-list ac line 4 permit tcp 171.0.0.0 255.0.0.0 any (hitcnt=0)
```

The **show access-list** command has the following line of output which shows the total number of cached ACL log flows (total), the number of cached deny-flows (denied), and the maximum number of allowed deny-flows:

```
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
```

Related Commands

access-group
access-list commit
access-list extended
access-list mode
clear access-group
clear access-list
configure
object-group
pager
show access-group
show access-list

access-list mode

To switch the compilation mode for the FWSM between manual- and auto-commit, use the **access-list mode** command.

access-list mode {**auto-commit** | **manual-commit**}

Syntax Description

auto-commit	Triggers ACL compilation immediately and automatically.
manual-commit	Specifies ACL compilation manually which takes effect only after the **access-list commit** command is entered.

Defaults

auto-commit.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

ACL commit allows you to change the ACL compilation behavior to synchronous compilation. The compilation mode is not saved as part of either the running or the saved configuration.

Both compilation methods behave the same way when downloading the new set of ACL rules. New ACL rules do not take effect (and the previous set of ACL rules still apply) until the new rules are completely downloaded and committed into the network processors. Traffic is not affected when a new set of rules is downloaded.

The manual-commit feature is designed for use by management applications.

Examples

This example shows how to modify an existing access list using the manual-commit mode without disrupting traffic:

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# no access-list old-acl
fwsm(config)# access-list old-acl …. : New ACE1
fwsm(config)# access-list old-acl …. : New ACE2
fwsm(config)# …….
fwsm(config)# access-list old-acl …. : New ACEn
fwsm(config)# access-list commit
```

This example shows how to delete the old access list and add a new one with a different name:

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# no access-list old-acl
fwsm(config)# access-list new-acl …. : New ACE1
fwsm(config)# access-list new-acl …. : New ACE2
fwsm(config)# …….
fwsm(config)# access-list new-acl …. : New ACEn
fwsm(config)# access-list commit
fwsm(config)# access-group new-acl in interface old-interface
```

The previous example shows that there is a slight traffic disruption on the old interface, which is equal to the time taken for the commit to complete and the **access-group** command to be applied in the last two command lines.

This example shows how to configure the access list as shown in the previous example without a traffic disruption:

```
fwsm(config)# access-list mode manual-commit
fwsm(config)# access-list new-acl …. : New ACE1
fwsm(config)# access-list new-acl …. : New ACE2
fwsm(config)# …….
fwsm(config)# access-list new-acl …. : New ACEn
fwsm(config)# access-list commit
fwsm(config)# access-group new-acl in interface old-interface
fwsm(config)# no access-list old-acl
fwsm(config)# access-list commit
```

The previous example shows that there is no disruption in traffic on the old interface. The only side effect of this sequence of commands is that the total number of ACEs configured on the FWSM will be NUM-ACE(old-acl) + NUM-ACE(new-acl) for a brief time.

This example shows how to use the manual-commit mode:

```
fwsm(config)# show access-list mode
ERROR: access-list <mode> does not exists
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
fwsm(config)# access-list commit
ERROR: access-list mode set to auto-commit; command ignored
fwsm(config)#
fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
```

```
fwsm(config)# access-list mode manual-commit
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
fwsm(config)# access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted addition)
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
ERROR: access-list not committed, ignoring command
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)#
fwsm(config)# access-group 1 in interface inside
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0)
fwsm(config)#
fwsm(config)# no access-list 1 permit ip any any
fwsm(config)#
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
access-list 1; 1 elements
access-list 1 extended permit ip any any (hitcnt=0) (uncommitted deletion)
fwsm(config)#
fwsm(config)# access-list commit
Access Rules Download Complete: Memory Utilization: < 1%
fwsm(config)# #
fwsm(config)# show access-list
access-list mode manual-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
300
fwsm(config)#
```

Related Commands

access-list commit
access-list extended
clear access-list
show access-list
show access-list mode

access-list object-group

To add an access list to the configuration and to configure policy for IP traffic through the firewall, use the **access-list object-group** command. To remove the access list, use the **no** form of this command.

[**no**] **access-list** *id* {**deny** | **permit**} **object-group** {*network_obj_grp_id destination_ip destination_mask*} [**log** [**disable** | [*level*] | **default**] | [**interval** *secs*]]

[**no**] **access-list** *id* {**deny** | **permit**} {**object-group** {*network_obj_grp_id* [*icmp_type* [*icmp_type_obj_grp_id*]]} [**log** [**disable** | [*level*] | **default**] | [**interval** *secs*]]

Syntax Description

id	Name or number of an access list.
deny	Denies access if the conditions are matched. See the "Usage Guidelines" section for the description.
permit	Permits access if the conditions are matched. See the "Usage Guidelines" section for the description.
network_obj_grp_id	Existing network object group identification.
destination_ip	IP address of the network or host to which the packet is being sent. See the "Usage Guidelines" section for additional information.
destination_mask	Netmask bits (mask) to be applied to *destination_ip* if the destination address is a network mask.
log disable | **default** | *level*	(Optional) Specifies that a syslog message 106100 is generated for the ACE. See the **log** command for information.
interval *secs*	Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds.
icmp_type	(Optional) ICMP type.
icmp_type_obj_grp_id	(Optional) Object group ICMP type ID.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for denied packets—Deny packets must be present to log denied packets.
- When the **log** optional keyword is specified, the default level for syslog message 106100 is 6 (informational).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear access-list** command automatically unbinds an access list from a **crypto map** command or interface. The unbinding of an access list from a **crypto map** command can lead to a condition that discards all packets because the **crypto map** commands referencing the access list are incomplete. To correct the condition, either define other **access-list** commands to complete the **crypto map** commands or remove the **crypto map** commands that pertain to the **access-list** command. Refer to the **crypto map client** command for more information.

ACLs that are dynamically updated on the FWSM by an AAA server can only be shown using the **show access-list** command. The **write** command does not save or display these updated lists.

The **access-list** command operates on a first-match basis.

If you specify an **access-list** command and bind it to an interface with the **access-group** command, by default, all traffic to that interface is denied. You must explicitly permit traffic. Inbound refers to traffic passing through the interface, not the traffic passing from a lower security level interface to a higher security level interface.

Always permit access first and then deny access afterward. If the host entries match, use the **permit** keyword; otherwise, use the default **deny** keyword. You only need to specify additional **deny** keywords if you need to deny specific hosts and permit everyone else.

You can see the security levels for interfaces with the **show nameif** command.

The optional ICMP message type (*icmp_type*) argument is ignored in IPSec applications because the message type cannot be negotiated with ISAKMP.

You can bind only one access list to an interface using the **access-group** command.

If you specify the **permit** optional keyword in the access list, the FWSM continues to process the packet. If you specify the **deny** optional keyword in the access list, the FWSM discards the packet and generates this syslog message:

```
%fwsm#-4-106019: IP packet from source_addr to destination_addr, protocol protocol
received from interface interface_name deny by access-group id
```

The **access-list** command uses the same syntax as the Cisco IOS software **access-list** command *except* that the FWSM uses a subnet mask. (Cisco IOS software uses a wildcard mask.) For example, in the Cisco IOS software **access-list** command, a subnet mask of 0.0.0.255 would be specified as 255.255.255.0 in the FWSM **access-list** command.

We recommend that you do not use the **access-list** command with the **outbound** command. Using these commands together may cause debugging issues. The **outbound** command operates from one interface to another and the **access-list** command when used with the **access-group** command applies only to a single interface. If you use these commands together, the FWSM evaluates the **access-list** command before checking the **outbound** command.

Refer to Chapter 3, “Managing Network Access and Use” in the *Cisco Firewall and VPN Configuration Guide* for a detailed description about using the **access-list** command to provide server access and to restrict outbound user access.

See the **aaa-server radius-acctport** and **aaa-server radius-authport** commands to verify or change port settings.

ICMP Message Types

For non-IPSec use only, if you prefer more selective ICMP access, you can specify a single ICMP message type as the last optional keyword in this command. Table 2-3 lists the possible ICMP types values.

Table 2-3 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	address-mask-request
18	address-mask-reply
31	conversion-error
32	mobile-redirect

Examples

This example shows how to set up an access list object group:

```
fwsm/contexta(config)# access-list VPN_SPLIT extended permit object-group ip host
209.165.200.225 host 10.1.1.1
```

This example shows how to display access list object group information:

```
FWSM(config)# show access-list
access-list mode auto-commit
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
```

Related Commands

access-group
access-list commit
access-list extended
access-list mode
clear access-group
clear access-list

configure
object-group
pager
show access-group
show access-list

access-list remark

To specify the text of the remark to add before or after an **access-list extended** command, use the **access-list remark** command. To delete the remark, use the **no** form of this command.

[**no**] **access-list** *id* **remark** *text*

Syntax Description

id	Name of an access list.
remark *text*	Specifies the text of the remark to add before or after an **access-list extended** command.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The remark text can be up to 100 characters in length, including spaces and punctuation.

On an ACL that includes a remark only, you cannot use the **access-group** command.

Examples

This example shows how to specify the text of the remark to add before or after an **access-list** command:

```
fwsm/context(config)# access-list 77 remark checklist
```

Related Commands

access-list extended
clear access-list
show access-list

access-list standard

To add an access list to the configuration and to configure the policy for IP traffic through the firewall, use the **access-list standard** command. To remove the access list, use the **no** form of this command.

[**no**] **access-list** *id* **standard** {**deny** | **permit**} {**any** | *ip_mask*}

Syntax Description

id	Name or number of an access list.
deny	Denies access if the conditions are matched. See the "Usage Guidelines" section for the description.
permit	Permits access if the conditions are matched. See the "Usage Guidelines" section for the description.
any	Specifies access to anyone.
ip_mask	Specific IP netmask.

Defaults

The defaults are as follows:

- The FWSM denies all packets on the originating interface unless you specifically permit access.
- ACL logging generates syslog message 106023 for denied packets—Deny packets must be present to log denied packets.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When used with the **access-group** command, the **deny** optional keyword does not allow a packet to traverse the FWSM. By default, the FWSM denies all packets on the originating interface unless you specifically permit access.

When you specify the *protocol* to match any Internet protocol, including TCP and UDP, use the **ip** keyword.

Refer to the **object-group** command for information on how to configure object groups.

You can use the **object-group** command to group access lists.

Use the following guidelines for specifying a source, local, or destination address:

- Use a 32-bit quantity in four-part, dotted-decimal format.
- Use the keyword **any** as an abbreviation for an address and mask of 0.0.0.0 0.0.0.0. We do not recommend that you use this keyword with IPSec.
- Use **host** *address* as an abbreviation for a mask of 255.255.255.255.

Examples

This example shows how to deny IP traffic through the firewall:

```
fwsm/context(config)# access-list 77 standard deny
```

This example shows how to permit IP traffic through the firewall if conditions are matched:

```
fwsm/context(config)# access-list 77 standard permit
```

Related Commands

object-group

activation-key

To change the activation key on the FWSM and check the activation key running on the FWSM against the activation key that is stored in the Flash partition of the FWSM, use the **activation-key** command.

activation-key *activation-key-four-tuple*

Syntax Description

activation-key-four-tuple	Activation key; see the "Usage Guidelines" section for formatting guidelines.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Enter the *activation-key-four-tuple* as a four-element hexadecimal string with one space between each element as follows:

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

The leading 0x specifier is optional; all values are assumed to be hexadecimal.

The key is not stored in the configuration file. The key is tied to the serial number.

Examples

This example shows how to change the activation key on the FWSM:

```
fwsm(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

Related Commands

clear activation-key
show activation-key
show version

admin-context

To set the administrator context, use the **admin-context** command.

admin-context *admin-context-name*

Syntax Description

admin-context-name	Context name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: Multiple

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The system requires one admin context to function properly. The admin context must reside on the disk. Until you create the admin context, no other contexts can be created. You can change the admin context to any other context using the **admin-context** command. However, the admin context must already exist and its configuration must reside on the disk before you make this change.

Examples

This example shows how to set the admin context on the FWSM:

```
fwsm(config)# admin-context test1
```

Related Commands

context
show admin-context
show context

alias

To translate one address into another, use the **alias** command. To disable a previously set **alias** command, use the **no** form of this command.

[**no**] **alias** {*interface_name*} *dnat_ip destination_ip* [*netmask*]

Syntax Description

interface_name	Internal network interface name that the destination_ip overwrites.
dnat_ip	IP address on the internal network that provides an alternate IP address for the external address that is the same as an address on the internal network.
destination_ip	IP address on the external network that has the same address as a host on the internal network.
netmask	(Optional) Network mask that is applied to both IP addresses.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When entering the *netmask*, enter **255.255.255.255** for host masks.

Use the **alias** command to prevent conflicts when you have IP addresses on a network that are the same as those on the Internet or another intranet. You can also use this command to do address translation on a destination address. For example, if a host sends a packet to 209.165.201.1, you can use the **alias** command to redirect traffic to another address, such as 209.165.201.30.

Note To ensure that DNS **fixup** works properly, disable **proxy-arp**. If you are using the **alias** command for DNS **fixup**, you can disable **proxy-arp** with the **sysopt noproxyarp** *internal_interface* command after the **alias** command has been executed.

After changing or removing an **alias** command, use the **clear xlate** command.

You must have an A (address) record in the DNS zone file for the “dnat” address in the **alias** command.

The **alias** command has two uses that can be summarized in the following ways:

- If the FWSM gets a packet that is destined for the *dnat_IP_address*, you can configure the **alias** command to send it to the *destination_ip_address*.

- If the FWSM gets a DNS packet that is returned to the FWSM destined for *destination_network_address*, you can configure the **alias** command to alter the DNS packet to change the destination network address to *dnat_network_address*.

The **alias** command automatically interacts with the DNS servers on your network to ensure that domain name access to the aliased IP address is handled transparently.

You can specify a net alias by using network addresses for the *destination_ip* and *dnat_ip* IP addresses. For example, the **alias 192.168.201.0 209.165.201.0 255.255.255.224** command creates aliases for each IP address between 209.165.201.1 and 209.165.201.30.

To access an **alias** *dnat_ip* address with **static** and **access-list** commands, specify the *dnat_ip* address in the **access-list** command as the address from which traffic is permitted as follows:

```
fwsm/context(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
fwsm/context(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
fwsm/context(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1
eq ftp-data
fwsm/context(config)# access-group acl_out in interface outside
```

An alias is specified with the inside address 192.168.201.1 mapping to the destination address 209.165.201.1.

When the inside network client 209.165.201.2 connects to example.com, the DNS response from an external DNS server to the internal client's query would be altered by the FWSM to be 192.168.201.29. If the FWSM uses 209.165.200.225 through 209.165.200.254 as the global pool IP addresses, the packet goes to the FWSM with SRC=209.165.201.2 and DST=192.168.201.29. The FWSM translates the address to SRC=209.165.200.254 and DST=209.165.201.29 on the outside.

Examples

This example shows that the inside network contains the IP address 209.165.201.29, which on the Internet belongs to example.com. When inside clients try to access example.com, the packets do not go to the FWSM because the client assumes that the 209.165.201.29 is on the local inside network.

To correct this, use the **alias** command as follows:

```
fwsm/context(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

fwsm/context(config)# show alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

This example shows a web server that is on the inside at 10.1.1.11 and the **static** command that was created at 209.165.201.11. The source host is on the outside with address 209.165.201.7. A DNS server on the outside has a record for www.example.com as follows:

```
dns-server# www.example.com. IN A 209.165.201.11
```

You must include the period at the end of the www.example.com. domain name.

This example shows how to use the **alias** command:

```
fwsm/context(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

The FWSM changes the name server replies to 10.1.1.11 for inside clients to directly connect to the web server.

To provide access, you also need the following commands:

```
fwsm/context(config)# static (inside,outside) 209.165.201.11 10.1.1.11

fwsm/context(config)# access-list acl_grp permit tcp host 209.165.201.7 host
209.165.201.11 eq telnet
```

```
fwsm/context(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

This example shows how to test the DNS entry for the host with the UNIX **nslookup** command:

```
fwsm(config)# nslookup -type=any www.example.com
```

Related Commands

access-list extended
static

allocate-acl-partition (context submode)

To map the current context to a partition, use the **allocate-acl-partition** command. To remove the context-to-partition mapping, use the **no** form of this command.

[**no**] **allocate-acl-partition** *partition-number*

Syntax Description

partition-number	Partition number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: Multiple

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When you run the **allocate-acl-partition Y** command, the current context is mapped to partition Y.

Using the **no allocate-acl-partition** command removes the mapping. If the context is the last context associated with the partition, the partition is moved from exclusive to non-exclusive . If the context is not the last context associated with the partition it is migrated to a non-exclusive partition.

Entering the **show allocate-acl-partition X** displays details about partition X. The details include the mode (non-exclusive/exclusive), and a list of associated contexts are displayed.

Examples

These examples show how to allocate contexts and ACL partitions.

This example shows how ACL partition #0 is shared by contexts “bandn” and “borders” while the remaining contexts share ACL paritition number 1:

```
FWSM/system# resource acl-partition 2
FWSM/system# context bandn
FWSM/system# allocate-acl-partition 0
FWSM/system# context borders
FWSM/system# allocate-acl-partition 0
FWSM/system# context mompopa
FWSM/system# context mompopb
FWSM/system# context mompopc
FWSM/system# context mompopd
```

This example shows how ACL partition 0 is given to context “bandn” exclusively. ACL partition 1 is given to context “borders” exclusively. The remaining customers are distributed among partitions 2 and 3 in a round-robin fashion.

```
FWSM/system# resource acl-partition 4
FWSM/system# context bandn
FWSM/system# allocate-acl-partition 0
FWSM/system# context borders
FWSM/system# allocate-acl-partition 1
FWSM/system# context mompopa
FWSM/system# context mompopb
FWSM/system# context mompopc
FWSM/system# context mompopd
```

Related Commands

resource acl-partition
resource-manager
show resource acl-partition
show resource allocation
show resource types
show resource usage

allocate-interface (context submode)

To assign VLAN interfaces to the context, after you enter the context submode, use the **allocate-interface** command. To remove the VLAN interfaces from the context, use the **no** form of this command.

[**no**] **allocate-interface vlan***number* [**-vlan***number*] [*mapped_name* [*-mapped_name*]]

Syntax Description

vlan*number*	Specifies the VLAN number.
-vlan*number*	(Optional) Specifies a VLAN number range.
mapped_name *-mapped_name*	(Optional) Alphanumeric alias for the VLAN interface that can be used within the context instead of the VLAN number.

Command Modes

Security Context Mode: Multiple

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Enter the **allocate-interface** command before you enter the **config-url (context submode)** command. The FWSM must assign VLAN interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (for example, the **nameif**, **nat**, **global**...commands). If you enter the **config-url (context submode)** command first, the FWSM loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

If you do not specify a mapped name, the VLAN number is used within the context.

For security purposes, you might not want the context administrator to know which VLANs are being used by the context. For example, instead of using the VLAN number in the **nameif** command, you must use the context mapped name.

If you enter the **no** form of **allocate-interface** command, all interface configuration in a context is removed.

If you specify a range of VLAN IDs, you can specify a matching range of context aliases. Follow these guidelines:

- The *mapped_name* must consist of an alphabetic portion followed by a numeric portion as follows:

  ```
  int0
  ```

- The alphabetic portion of the *mapped_name* must match for both ends of the range as follows:

  ```
  vlan2-vlan10
  ```

- The numeric portion of the *mapped_name* must include the same amount of numbers as the **vlanx-vlany** entry. For example, both ranges include 100 interfaces:

```
fwsm/context(config)# allocate-interface vlan100-vlan199 int1-int100
```

- Do not include a space between the **vlan** keyword and the number.

If you enter **vlan100-vlan199 int1-int15**, or **vlan100-vlan199 happy1-sad5**, the command fails.

An additional context subconfiguration mode command is the **config-url (context submode)** command.

Examples

This example shows how to assign VLAN interfaces to the context:

```
fwsm(config)# context test1
Creating context 'test1'... Done.(3)
fwsm/context(config)# allocate-interface vlan5
fwsm/context(config)# allocate-interface vlan6-vlan10
```

Related Commands

admin-context
changeto
class
clear context
config-url (context submode)
show context

area

To configure a regular OSPF area, use the **area** command. The **area** command is a subcommand of the **router ospf** command. To remove configured areas, use the **no** form of this command.

[**no**] **area** *area_id* {**authentication** [**message-digest**]} | {**default-cost** *cost*} | {**filter-list prefix** {*prefix_list_name* **in | out**}} | {**range** *ip_address netmask* [**advertise | not-advertise**]}

[**no**] **area** *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type 1 | 2**] [**metric** *metric_value*]] [**no-summary**]

area *area_id* **stub** [**no-summary**]

[**no**] **area** *area_id* {**virtual-link** *router_id*} [**authentication** [**message-digest | null**]] [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**authentication-key** *password*] [**message-digest-key** *id* **md5** *password*]

Syntax Description

area_id	Regular OSPF area.
authentication	Specifies the authentication type.
message-digest	(Optional) Specifies the message digest authentication that is used.
default-cost *cost*	Specifies the cost for the default summary route that is used for a stub or NSSA from 0 to 65535. The default value for *cost* is 1.
filter-list prefix *prefix_list_name*	Specifies the name of a prefix list.
in	Applies the configured prefix list to prefixes advertised inbound to the specified area.
out	Applies the configured prefix list to prefixes advertised outbound from the specified area.
range *ip_address*	Specifies the router ID in IP address format.
netmask	IP address mask or IP subnet mask used for a summary route.
advertise	(Optional) Sets the address range status to advertise and generates type 3 summary link-state advertisements (LSAs).
not-advertise	(Optional) Sets the address range status to DoNotAdvertise. The type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.
nssa	Specifies the not-so-stubby area.
no-redistribution	(Optional) Imports route only into the normal areas and not into the NSSA area.
default-information -originate	(Optional) Generates a type 7 default in the NSSA area.
metric-type 1 | 2	(Optional) Specifies the metric type as type **1** or type **2**.
metric *metric_value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
no-summary	(Optional) Prevents an area border router (ABR) from sending summary LSAs into the stub area.
stub	Specifies that this OSPF area carries a default route and intra- and inter-area routes but does not carry external routes.

virtual-link *router-id*	Configures the router ID for an OSPF process.
null	(Optional) Specifies that no authentication is used. Overrides password or message digest authentication if configured for the OSPF area.
hello-interval *seconds*	(Optional) Specifies the interval between hello packets sent on the interface; valid values are from 1 to 65535 seconds.
retransmit-interval *seconds*	(Optional) Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
transmit-delay *seconds*	(Optional) Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535. The default is 5 seconds.
dead-interval *seconds*	(Optional) Specifies the interval before declaring a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
authentication-key *password*	(Optional) Specifies an OSPF authentication password for use by neighboring routing devices.
message-digest-key *key_id*	(Optional) Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
md5 *password*	(Optional) Specifies an alphanumeric password up to 16 bytes.

Defaults

The defaults are as follows:

- OSPF routing is disabled on the FWSM.
- The *cost* is 1.
- The authentication type for an area is **0**, which means that there is no authentication.
- OSPF routing through the FWSM is compatible with RFC 1583.
- The **area** *area_id* **range** *ip_address netmask* [**advertise | not-advertise**] command is **advertise**.
- The **dead-interval** is four times the interval set by the **ospf hello-interval** command.
- The **hello-interval** *seconds* is 10 seconds.
- The **retransmit-interval** *seconds* is 5 seconds.
- The **transmit-delay** *seconds* is 1 second.
- No area is defined for the **area** *area_id* **nssa** [[**no-redistribution**] [**default-information-originate**][**no-summary**]] command.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF protocol is used instead of the Routing Information Protocol (RIP). Do not attempt to configure the FWSM for both OSPF and RIP simultaneously.

The **router ospf** command is the global configuration command for OSPF routing processes running on the FWSM. This is the main command for all of the OSPF configuration commands.

Once you enter the **router ospf** command, the command prompt appears as (config-router)#, indicating that you are in the submode.

When you configure the area_id, the guidelines are as follows:

- For all contexts, you can specify an *area_id* as either a decimal value or as an IP address.
- The ID is the area that is to be associated with the OSPF address range. If you associate areas with IP subnets, you can specify a subnet address as the *area_id*.
- When used in the context of authentication, *area_id* is the identifier of the area on which authentication is to be enabled.
- When used in a cost context, *area_id* is the identifier for the stub or NSSA.
- When used in the context of a prefix list, *area_id* is the identifier of the area on which filtering is configured.
- When used in a stub area or not-so-stubby area (NSSA) context, *area_id* is the identifier for the stub or NSSA area.
- When used in the context of an area range, *area_id* is the identifier of the area at whose boundary it is to summarize routes.

The **area** *area_id* subcommand creates a regular OSPF area. The **no area** *area_id* command removes the OSPF area, whether it is regular, stubby, or not so stubby.

```
fwsm(config)# area area_id authentication message-digest
```

The default authentication type for an area is **0**, which indicates no authentication. To enable authentication for an OSPF area, use the **area** *area_id* **authentication message-digest** subcommand. To remove an authentication configuration from an area, use the **no area** *area_id* **authentication message-digest** subcommand.

```
fwsm(config)# area area_id default-cost cost
```

To specify a cost for the default summary route sent into a stub or not-so-stubby area (NSSA), use the **area** *area_id* **default-cost** *cost* subcommand. To remove the assigned default route cost, use the **no area** *area_id* **default-cost** subcommand. The default value for *cost* is 1.

```
fwsm(config)#  area area_id filter-list prefix prefix_list_name in
```

To filter prefixes advertised in type 3 LSAs between OSPF areas of an ABR, use the **area** *area_id* **filter-list prefix** *prefix_list_name* [**in | out**] subcommand. To change or cancel the filter, use the **no area** *area_id* **filter-list prefix** *prefix_list_name* [**in | out**] subcommand.

Routes that originate from other routing protocols (or different OSPF processes) and that are injected into OSPF through redistribution are called external routes. There are two forms of external metrics: type 1 and type 2. These routes are represented by `O E2` (for type 2) or `O E1` (for type 1) in the IP routing table, and they are examined by the FWSM after it finishes building its internal routing table. After the routes are examined, they are flooded unaltered throughout the autonomous systems. (Autonomous systems are a collection of networks that are subdivided by areas under a common administration sharing a common routing strategy.)

OSPF type 1 metrics result in routes that add the internal OSPF metric to the external route metric; they are also expressed in the same terms as an OSPF link-state metric. The internal OSPF metric is the total cost of reaching the external destination including whatever internal OSPF network costs are incurred to get there. These costs are calculated by the device wanting to reach the external route. Because the cost is calculated this way, the OSPF type 1 metric is preferred.

OSPF type 2 metrics do not add the internal OSPF metric to the cost of external routes and are the default type used by OSPF. The use of OSPF type 2 metrics assumes that you are routing between autonomous systems. The cost is considered greater than any internal metrics, which eliminates the need to add internal OSPF metrics.

The **default-information-originate** optional keyword takes effect on an NSSA ABR or an NSSA autonomous system boundary router (ASBR) only.

To configure an NSSA area, use the **area** *area_id* **nssa** [**no-redistribution**] [**default-information-originate** [**metric-type 1 | 2**] [**metric** *metric_value*]] [**no-summary**] subcommand. To remove the entire NSSA configuration, use the **no area** *area_id* **nssa** subcommand. To remove a single NSSA configuration optional keyword, specify the optional keyword in the **no** subcommand. For example, to remove the **no-redistribution** optional keyword, use the **no area** *area_id* **nssa no-redistribution** command. By default, no NSSA is defined.

```
fwsm(config)# area area_id range address netmask advertise | not-advertise
```

To consolidate and summarize routes at an area boundary, use the **area** *area_id* **range** *address netmask* [**advertise | not-advertise**] subcommand. To disable this function, use the **no area** *area_id* **range** *ip_address netmask* subcommand. The **no area** *area_id* **range** *ip_address netmask* **not-advertise** subcommand removes only the **not-advertise** optional keyword.

```
fwsm(config)# area area_id stub no-summary
```

To define an area as a stub area, use the **area** *area_id* **stub** [**no-summary**] subcommand. To remove the stub area function, use the **no area** *area_id* **stub** [**no-summary**] subcommand. When **area** *area_id* **stub no-summary** is configured, you must use the **no area** *area_id* **stub no-summary** subcommand to remove the **no summary** optional keyword. The default is for no stub areas to be defined.

You cannot configure virtual links across a stub area, and they cannot contain an ASBR.

To define an OSPF virtual link, use the **area** *area_id* **virtual-link** *router-id* subcommand with the optional parameters. To remove a virtual link, use the **no area** *area_id* **virtual-link** *router_id* subcommand.

Examples

This example shows how to use the **area** commands:

```
fwsm/context(config)# area authentication
```

Related Commands

router ospf
show area

arp

To add a static ARP entry and set the ARP persistence timer, use the **arp** command. To disable ARP inspection or remove the ARP cache timeout from the configuration, use the **no** form of this command.

[**no**] **arp** *interface_name ip_addr mac_addr* [**alias**]

[**no**] **arp timeout** *seconds*

Syntax Description

interface_name	Interface name whose ARP table will be changed or viewed.
ip_addr	IP address for an ARP table entry.
mac_addr	Hardware MAC address for the ARP table entry.
alias	(Optional) Configures a static proxy ARP mapping (proxied IP-to-physical address binding) for the addresses specified.
timeout *seconds*	Specifies the duration to wait before the ARP table rebuilds itself and automatically updates new host information.

Defaults

The defaults are as follows:

- Proxy ARP is enabled on all interfaces.
- The ARP persistence timer is 14400 seconds (4 hours).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The ARP maps an IP address to a MAC address (for example, 00e0.1e4e.3d8b) and is defined in RFC 826. Proxy ARP is a variation of the ARP protocol in which an intermediate device (for example, the FWSM) sends an ARP response on behalf of an end node to the requesting host. ARP mapping occurs automatically as the FWSM processes traffic; however, you can configure the ARP cache timeout value, static ARP table entries, or proxy ARP. The maximum ARP cache timeout value is 3567587 seconds.

Note Because ARP is a low-level TCP/IP protocol that resolves a node's MAC (physical) address from its IP address (through an ARP request asking the node with a particular IP address to send back its physical address), the presence of entries in the ARP cache indicates that the FWSM has network connectivity.

The **arp timeout** command specifies the duration to wait before the ARP table rebuilds itself, automatically updating host information. This feature is also known as the ARP persistence timer. The **no arp timeout** command resets the ARP persistence timer to its default value.

The **arp** *interface_name ip mac* command adds a static (persistent) entry to the FWSM ARP cache. For example, you could use the **arp** *interface_name ip mac* command to set up a static IP-to-MAC address mapping for hosts on your network. Use the **no arp** *interface_name ip mac* command to remove the static ARP mapping.

The static **arp** entries and the **arp alias** entries are not cleared when the ARP persistence timer times out and are automatically stored in the configuration when you use the **write** command to store the configuration.

The **arp** *interface_name ip mac* **alias** command configures proxy ARP for the IP and MAC addresses specified. Enable proxy ARP you allow the host to another host at that IP address. The FWSM is an intermediary between the two hosts so by sending the packet to the FWSM, the FWSM will pass the packet to the designated host. The FWSM returns the MAC address of the FWSM in the proxied response. Use the **no arp** *interface_name ip mac* **alias** command to remove the static proxy ARP mapping.

The *interface_name argument* is specified by the **nameif** command.

Examples

These examples show how to configure ARP:

```
fwsm/context(config)# arp inside 192.168.0.42 00e0.1e4e.2a7c
fwsm/context(config)# arp outside 192.168.0.43 00e0.1e4e.3d8b alias
fwsm/context(config)# arp timeout 60

fwsm/context(config)# show arp stat
Number of ARP entries:

PIX   270
NP1   269
NP2   269

NP_IPPS_ADD_ARP_ENTRY_NP_count          = 538
NP_IPPS_UPDATE_ARP_ENTRY_NP_count       = 4
NP_IPPS_DELETE_ARP_ENTRY_NP_count       = 0
NP_IPPS_ADD_ARP_ENTRY_NP_resend_count           = 0
NP_IPPS_UPDATE_ARP_ENTRY_NP_resend_count        = 0
NP_IPPS_DELETE_ARP_ENTRY_NP_resend_count        = 0
NP_IPPS_ADD_ARP_ENTRY_NP_failed_count           = 0
NP_IPPS_UPDATE_ARP_ENTRY_NP_failed_count        = 0
NP_IPPS_DELETE_ARP_ENTRY_NP_failed_count        = 0
arp_miss_counter                = 310
arp_miss_invalid_vcid   = 0
        Dropped blocks in ARP: 0
        Maximum Queued blocks: 1
        Queued blocks: 0
        Interface collision ARPs Received: 0
        ARP-defense Gratuitous ARPS sent: 0
        Total ARP retries: 0
        Unresolved hosts: 0
        Maximum Unresolved hosts: 11
```

Related Commands

clear arp
show arp
sysopt

arp-inspection

To enable or disable Address Resolution Protocol (ARP) inspection on an interface, use the **arp-inspection** command. To remove ARP inspection, use the **no** form of this command.

[**no**] **arp-inspection** *if_name* **enable** [**flood** | **no-flood**]

Syntax Description

if_name	Interface name whose ARP table will be changed or viewed.
enable	Enables ARP inspection on the interface.
flood	(Optional) ARP forwarding is on for the interface.
no-flood	(Optional) Specifies that ARP forwarding is off for the interface.

Defaults

ARP inspection is disabled on all interfaces.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Transparent

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To add static ARP entries in the FWSM this command is used to add bindings between IP addresses and MAC addresses for ARP inspection.

ARP inspection is enabled per interface and is configurable to flood or no flood depending on whether there is a miss or a hit in the static ARP table, when ARP inspection is enabled on the interface. This command also allows you to turn ARP forwarding on or off for an interface.

If ARP inspection is enabled on an interface, all ARP packets (reply or gratuitous arp) from this interface are inspected before forwarding. The ARP inspection check in for the static ARP table is as follows:

- If an entry is found and the entry matches, the packet is forwarded.
- If an entry is found but there is an entry mismatch, the packet is dropped and a syslog message is generated.
- If an entry does not exist and the flood option is enabled, the packet is forward to the correct interface.
- If an entry does not exist and the no_flood option is enabled, the packet is dropped and a syslog message is generated.

Examples

This example shows how to configure an ARP inspection:

```
fwsm/context(config)# arp-inspection
```

Related Commands

clear arp
show arp
sysopt

auth-prompt

To change the AAA challenge text for HTTP, FTP, and Telnet access, use the **auth-prompt** command. To disable the challenge text, use the **no** form of this command.

[**no**] **auth-prompt** [**prompt** | **accept** | **reject**] *prompt text*

Syntax Description

prompt	(Optional) Specifies the AAA challenge prompt string.
accept	(Optional) Displays the prompt *string* if a user authentication through Telnet is accepted.
reject	(Optional) Displays the prompt *string* if a user authentication through Telnet is rejected.
prompt text	String up to 235 alphanumeric characters or 31 words, limited by whichever maximum is first reached.

Defaults

The defaults are as follows:

- Microsoft Internet Explorer displays only up to 37 characters in an authentication prompt.
- Netscape Navigator displays up to 120 characters.
- Telnet and FTP display up to 235 characters in an authentication prompt.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The AAA challenge text displays when a user logs in. If you do not use the AAA challenge text command, the following is displayed above the username and password prompts:

- FTP users see “FTP authentication”
- HTTP users see “HTTP Authentication”
- The challenge text does not appear for Telnet access

If the user authentication occurs from Telnet, you can use the **accept** and **reject** optional keywords to display different authentication prompts if the authentication attempt is accepted or rejected by the authentication server.

You should not use special characters when you change the challenge text; however, spaces and punctuation characters are permitted. Entering a question mark or pressing the **Enter** key ends the string. (The question mark appears in the string.)

Examples

This example shows how to set the authentication prompt and how users see the prompt:

```
fwsm/context(config)# auth-prompt XYZ Company Firewall Access
```

After this string is added to the configuration, users see the following:

```
Example.com Company Firewall Access
User Name:
Password:
```

Note The **prompt** keyword can be included or omitted.

This example shows how to set the authentication prompt using the prompt keyword:

```
fwsm/context(config)# auth-prompt prompt Hello There!
```

This example shows how to set the authentication prompt without the prompt keyword:

```
fwsm/context(config)# auth-prompt Hello There!
```

Related Commands

aaa authentication
auth-prompt
clear auth-prompt
show auth-prompt

banner

To configure the session, login, or message-of-the-day banner, use the **banner** command. To remove all the lines for the banner optional keyword specified, use the **no** form of this command.

[**no**] **banner** {**exec | login | motd** *text*}

Syntax Description

exec	Configures the system to display a banner before displaying the enable prompt.
login	Configures the system to display a banner before the password login prompt when accessing the FWSM using Telnet.
motd	Configures the system to display a message-of-the-day banner.
text	Line of message text to be displayed in the FWSM CLI.

Defaults

The default is no login, session, or message-of-the-day banner.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **banner** command configures a banner to display for the optional keyword specified. The *text* string consists of all characters following the first white space (space) until the end of the line (carriage return or line feed [LF]). Spaces in the text are preserved. However, you cannot enter tabs through the CLI.

Subsequent *text* entries are added to the end of an existing banner unless the banner is cleared first.

Note The tokens $(domain) and $(hostname) are replaced with the host name and domain name of the FWSM. When you enter a $(system) token in a context configuration, the context uses the banner configured in the system configuration.

Multiple lines in a banner are handled by entering a new banner command for each line that you wish to add. Each line is then appended to the end of the existing banner. If the text is empty, a carriage return (CR) is added to the banner. There is no limit on the length of a banner other than RAM and Flash limits.

When accessing the FWSM through Telnet or SSH, the session closes if not enough system memory is available to process the banner messages or if a TCP write error occurs.

To replace a banner, use the **no banner** command before adding the new lines.

Use the **no banner** {**exec | login | motd**} command to remove all the lines for the banner optional keyword specified.

The **no banner** command does not selectively delete text strings, so any *text* that you enter at the end of the **no banner** command is ignored.

Examples

This example shows how to configure the **motd**, **exec**, and **login** banners:

```
fwsm(config)# banner motd Think on These Things
fwsm(config)# banner exec Enter your password carefully
fwsm(config)# banner login Enter your password to log in
fwsm(config)# show banner
exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

This example shows how to add a second line to a banner:

```
fwsm(config)# banner motd and Enjoy Today
fwsm(config)# show banner motd
Think on These Things
and Enjoy Today
```

Related Commands

clear banner
enable
login
password/passwd
show banner
ssh
telnet

ca authenticate

To allow the FWSM to authenticate its certification authority (CA) by obtaining the CA's self-signed certificate, which contains the CA's public key, use the **ca authenticate** command.

ca authenticate *ca_nickname* [*fingerprint*]

Syntax Description

ca_nickname	Name of the certification authority (CA).
fingerprint	(Optional) Key consisting of alphanumeric characters that the FWSM uses to authenticate the CA's certificate.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. If you previously declared the CA and want to update its characteristics, specify the name you previously created. The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

The FWSM supports the CA servers from VeriSign, Entrust, Baltimore Technologies, and Microsoft.

The certificate lifetime and the certificate revocation list (CRL) are checked in coordinated universal time (UTC). The FWSM clock is synchronized with the switch. This clock setting determines the certificate lifetime and revocation.

The FWSM authenticates the entity certificate (the device certificate). The FWSM assumes that the certificate is issued by the same trusted point or root (the CA server). As a result, the trusted point or root should have the same root certificate (issuer certificate). The FWSM assumes that the entity exchanges the entity certificate only and cannot process a certificate chain that includes both the entity and root certificates.

To authenticate a peer's certificate(s), the FWSM must obtain the CA certificate containing the CA public key. Because the CA certificate is a self-signed certificate, you should authenticate the key manually by contacting the CA administrator. You can authenticate the public key in that certificate by including the key's fingerprint within the **ca authenticate** command. The FWSM will discard the received CA certificate and generate an error message if the fingerprint that you specified is different from the received one. You can also compare the two fingerprints without entering the key within the command.

If you are using RA mode (within the **ca configure** command), when you issue the **ca authenticate** command, the RA signing and encryption certificates and the CA certificate are returned from the CA.

The **ca authenticate** command is not saved to the FWSM configuration. However, the public keys that are embedded in the received CA (and RA) certificates are saved in the configuration as part of the RSA public key record (called the "RSA public key chain"). To save the public keys permanently to the Flash partition, use the **ca save all** command. To see the CA's certificate, use the **show ca certificate** command.

Note If the CA does not respond by a timeout period after this command is entered, the terminal control is returned so that it is not tied up. In this situation, you must reenter the command.

Examples

This example shows that a request for the CA's certificate was sent to the CA. The fingerprint was not included in the command. The CA sends its certificate and the FWSM prompts for verification of the CA's certificate by checking the CA certificate's fingerprint. If both fingerprints match, then the certificate is considered valid.

```
fwsm/context_name(config)# ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
```

This example shows the error message. The fingerprint is included in the command. The two fingerprints do not match, and therefore the certificate is not valid.

```
fwsm/context_name(config)# ca authenticate myca 0123456789ABCDEF0123
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 5432
%Error in verifying the received fingerprint. Type help or '?' for a list of
available commands.
```

Related Commands

show ca

ca configure

To specify the communication parameters between the FWSM and the CA, use the **ca configure** command. To return to the default settings, use the **no** form of this command.

[**no**] **ca configure** *ca_nickname* {**ca** | **ra**} *retry_period retry_count* [**crloptional**]

Syntax Description

ca_nickname	Name of the certification authority (CA).
ca	Contacts the CA.
ra	Contacts the registration authority (RA).
retry_period	Number of minutes that the FWSM waits before resending a certificate request to the CA when it does not receive a response from the CA to its previous request; valid values are from 1 to 60 minutes.
retry_count	How many times that the FWSM will resend a certificate request when it does not receive a certificate from the CA from the previous request; valid values are from 1 to 100.
crloptional	(Optional) Allows other peers' certificates to be accepted by the FWSM even if the appropriate certificate revocation list (CRL) is not accessible to the FWSM.

Defaults

The defaults are as follows:

- The *retry_period* is 1 minute.
- The *retry_count* is 0 (there is no limit to the number of times that the FWSM should contact the CA to obtain a pending certificate).
- The default is without the **crloptional** optional keyword.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. If you previously declared the CA and want to update its characteristics, specify the name that you previously created. The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

Examples

This example shows that *myca* is the name of the CA and that the CA is contacted rather than the RA. It also indicates that the FWSM will wait 5 minutes before sending another certificate request, if it does not receive a response, and will resend a total of 15 times before dropping its request. If the CRL is not accessible, **crloptional** tells the FWSM to accept other peer's certificates.

```
fwsm/context_name(config)# ca configure myca ca 5 15 crloptional
```

Related Commands

ca authenticate
show ca

ca crl request

To allow the FWSM to obtain an updated CRL from the CA at any time, use the **ca crl request** command. To delete the CRL from the FWSM, use the **no** form of this command.

[**no**] **ca crl request** *ca_nickname*

Syntax Description

ca_nickname	Name of the certification authority (CA).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. If you previously declared the CA and want to update its characteristics, specify the name you previously created. The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

A CRL lists all the network devices certificates that have been revoked. The FWSM will not accept revoked certificates; any peer with a revoked certificate cannot exchange IPSec traffic with the FWSM.

The first time that the FWSM receives a certificate from a peer, it downloads a CRL from the CA. The FWSM then checks the CRL to make sure that the peer's certificate has not been revoked. If the certificate appears on the CRL, it will not accept the certificate and will not authenticate the peer.

A CRL can be reused with subsequent certificates until the CRL expires. When the CRL expires, the FWSM automatically updates it by downloading a new CRL and replaces the expired CRL with the new CRL.

If the FWSM has a CRL that has not yet expired, but you suspect that the CRL's contents are out of date, use the **ca crl request** command to request that the latest CRL is downloaded to replace the old CRL.

The **ca crl request** command is not saved with the FWSM configuration between reloads.

The **show ca crl** command allows you to know whether there is a CRL in RAM, and where and when the CRL is downloaded.

Examples

This example shows how the FWSM obtains an updated CRL from the CA with the name myca:

```
fwsm/context_name(config)# ca crl request myca
```

Related Commands

ca authenticate
show ca

ca enroll

To send an enrollment request to the CA requesting a certificate for all of the FWSM's key pairs, use the **ca enroll** command. To cancel the current enrollment request, use the **no** form of this command.

[**no**] **ca enroll** *ca_nickname challenge_password* [**serial**] [**ipaddress**]

Syntax Description

ca_nickname	Name of the certification authority (CA).
challenge_password	Required password that gives the CA administrator some authentication when a user calls to ask for a certificate to be revoked; the password can be up to 80 characters.
serial	(Optional) Returns the FWSM's serial number in the certificate.
ipaddress	(Optional) Returns the FWSM's IP address in the certificate.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can enter any string for *ca_nickname*. (If you previously declared the CA and want to update its characteristics, specify the name that you previously created.) The CA might require a particular name, such as its domain name.

The FWSM supports only one CA at a time.

You can use the **ca enroll** command to send an enrollment request to the CA requesting a certificate for all of the FWSM's key pairs. This action is also known as "enrolling" with the CA.

The FWSM needs a signed certificate from the CA for each of its RSA key pairs. If you previously generated general-purpose keys, entering the **ca enroll** command obtains one certificate corresponding to the one general-purpose RSA key pair. If you previously generated special usage keys, entering this command obtains two certificates corresponding to each of the special-usage RSA key pairs.

If you already have a certificate for the keys, you will not be able to complete this command; instead, you are prompted to remove the existing certificate first.

The **ca enroll** command is not saved with the FWSM configuration between reloads. To verify if the enrollment process succeeded and to display the FWSM's certificate, use the **show ca certificate** command.

The required challenge password is necessary in the event that you need to revoke the FWSM's certificate(s). When you ask the CA administrator to revoke the certificate, you must supply this challenge password as a protection against fraudulent or mistaken revocation requests.

Note Do not forget the password; this password is not stored in memory anywhere.

If you lose the password, the CA administrator may still be able to revoke the FWSM's certificate but will require further manual authentication of the FWSM administrator identity.

The FWSM's serial number is optional. If you provide the **serial** optional keyword, the serial number is included in the obtained certificate. The serial number is not used by IPSec or Internet Key Exchange (IKE) but may be used by the CA to either authenticate certificates or to later associate a certificate with a particular device. Ask the CA administrator if serial numbers should be included in the certificate. If you are in doubt, specify the **serial** optional keyword.

The FWSM's IP address is optional. If you enter the **ipaddress** optional keyword, the IP address is included in the obtained certificate. Normally, you do not include the **ipaddress** optional keyword because the IP address binds the certificate to a specific entity. If you move the FWSM, you need to issue a new certificate.

Note When configuring ISAKMP for certificate-based authentication, you should match the ISAKMP identity type with the certificate type. Enter the **ca enroll** command to obtain a certificate with the identity based on the host name. Enter the **isakmp identity** command to obtain a certificate based on the address instead of the host name. You can reconcile this disparity of identity types by using the **isakmp identity address** command. See the **isakmp** command for information about the **isakmp identity address** command.

Examples

This example shows how the FWSM sends an enrollment request to the CA myca.example.com:

```
fwsm/context_name(config)# ca enroll myca.example.com 1234567890 serial
```

Related Commands

ca authenticate
show ca

ca generate rsa

To generate the RSA key pairs for your FWSM, use the **ca generate rsa** command.

ca generate rsa {**key** | **specialkey**} *key_modulus_size*

Syntax Description

key	Generates an RSA key for the FWSM.
specialkey	Generates two special-purpose RSA key pairs instead of one general-purpose key.
key_modulus_size	Modulus used to generate the RSA key in a size measured in bits; valid values are **512**, **768**, **1024**, and **2048** bits.

Note Before using this command, make sure that your Firewall Services Module host name and domain name have been configured (using the **hostname** and **domain-name** commands). If a domain name is not configured, the FWSM uses a default domain of ciscopix.com.

Defaults

The defaults are as follows:

- The RSA key modulus default (during PDM setup) is **768**.
- The default domain is ciscofwsm.com.

Command Modes

Configuration mode.

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

RSA keys are generated in pairs—one public RSA key and one private RSA key

If your FWSM already has RSA keys when you use this command, you are warned and prompted to replace the existing keys with new keys.

Note The larger the key modulus size that you specify, the longer it takes to generate an RSA. We recommend a default value of 768.

PDM uses the Secure Socket Layer (SSL) communications protocol to communicate with the firewall.

SSL uses the private key generated with the **ca generate rsa** command. For a certificate, SSL uses the key obtained from a certification authority (CA). If that does not exist, it uses the FWSM self-signed certificate that was created when the RSA key pair was generated.

The **ca generate rsa** command is not saved in the FWSM configuration. However, the keys generated by this command are saved in a persistent data file in the Flash partition, which you can save with the **ca save all** command and view with the **show ca my rsa key** command.

Examples

This example shows how one general-purpose RSA key pair is generated. The selected size of the key modulus is 1024.

```
fwsm(config) ca generate rsa key 1024
Key name:firewall.cisco.com
 Usage:General Purpose Key
 Key Data:
  30819f30 0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c8ed4c
  9f5e0b52 aea931df 04db2872 5c4c0afd 9bd0920b 5e30de82 63d834ac f2e1db1f
  1047481a 17be5a01 851835f6 18af8e22 45304d53 12584b9c 2f48fad5 31e1be5a
  bb2ddc46 2841b63b f92cb3f9 8de7cb01 d7ea4057 7bb44b4c a64a9cf0 efaacd42
  e291e4ea 67efbf6c 90348b75 320d7fd3 c573037a ddb2dde8 00df782c 39020301 0001
```

Related Commands

show ca

ca identity

To declare the CA that the FWSM uses, use the **ca identity** command. To remove the **ca identity** command from the configuration and delete all the certificates that are issued by the specified CA and CRLs, use the **no** form of this command.

[**no**] **ca identity** *ca_nickname* [*ca_ipaddress* | *hostname* [**:***ca_script_location*] [*ldap_ip address* | *hostname*]]

Syntax Description

ca_nickname	Name of the certification authority (CA).
ca_ipaddress	(Optional) CA's IP address.
hostname	(Optional) Host name.
:*ca_script_location*	(Optional) Location and script on the CA server.
ldap_ipaddress	(Optional) IP address of the Lightweight Directory Access Protocol (LDAP) server.

Defaults

The defaults are as follows:

- **:***ca_script_location*—The location and script on the CA server is /cgi-bin/pkiclient.exe.
- *ldap_ipaddress*—Querying of a certificate or a CRL is done through Cisco's PKI protocol.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the CA supports LDAP, the query functions may also use LDAP.

The FWSM supports one CA at one time.

If the CA administrator has not put the CGI script in this location, you need to provide the location and the name of the script in the **ca identity** command.

The FWSM uses a subset of the HTTP protocol to contact the CA and must identify a particular cgi-bin script to handle CA requests. The default location and script on the CA server is /cgi-bin/pkiclient.exe. If the CA administrator has not put the CGI script in the previously listed location, you need to include the location and the name of the script within the **ca identity** command.

By default, querying a certificate or a CRL is done through the Cisco's PKI protocol. If the CA supports the Lightweight Directory Access Protocol (LDAP), the query functions may use LDAP. You must include the IP address of the LDAP server within the **ca identity** command.

Examples

This example shows that the CA myca.example.com is declared as the FWSM's supported CA. The CA's IP address of 205.139.94.231 is provided.

```
fwsm/context_name(config)# ca identity myca.example.com 205.139.94.231
```

Related Commands

show ca

ca save all

To save the FWSM's RSA key pairs, the CA, RA, and FWSM's certificates, and the CA's CRLs in the persistent data file in the Flash partition between reloads, use the **ca save all** command. To remove the saved data from the FWSM's Flash partition, use the **no** form of this command.

[**no**] **ca save all**

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **ca save** command is not saved with the FWSM configuration between reloads.

To see the current status of the requested certificates and relevant information of the received certificates, use the **show ca certificate** command. Because the certificates contain no sensitive data, any user can issue this **show** command.

Examples

This command shows how to save the FWSM RSA key pairs:

```
fwsm/context_name(config)# ca save all
```

Related Commands

show ca

ca subject-name

To create the device certificate with the subject distinguished name (DN), use the **ca subject-name** command. To remove the subject names, use the **no** form of this command.

[**no**] **ca subject-name** *ca_nickname X.500_string*

Syntax Description

ca_nickname	Name of the certification authority (CA).
X.500_string	Character string indicating the DN sent.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Specify the *X.500_string* using the RFC 1779 format.

The **ca subject-name** *ca_nickname X.500_string* command is a certificate enrollment enhancement that supports X.500 directory names.

When the **ca subject-name** *ca_nickname X.500_string* command is configured, the FWSM enrolls the device certificate with the subject DN that is specified in the *X.500_string* using the RFC 1779 format. The supported DN attributes are listed in Table 2-4.

Table 2-4 Supported DN Attributes

Attribute	Description
`ou`	Organizational Unit Name
`o`	Organization Name
`st`	State or Province Name
`c`	Country Name
`ea`	E-mail address (a non-RFC 1779 format attribute)

For more information on RFC 1779, refer to http://www.ietf.org/rfc/rfc1779.txt.

FWSM software version 2.2(1) supports X.509 (certificate support) on the VPN client. The Cisco IOS software, the VPN 3000 concentrator, and the FWSM look for the correct VPN group (mode configuration group) according to the "ou" attribute. (The "ou" attribute is part of the subject DN of the device certificate when the Easy VPN client negotiates the RSA signature.)

Note If you use the *X.500_string* to communicate between a Cisco VPN 3000 head end and the FWSM, you must not configure the VPN 3000 head end to use DNS names for the backup servers. Instead, you must specify the backup servers by their IP addresses.

Examples

This example shows how to create the device certificate with the subject DN (where my_department is the VPN group):

```
fwsm/context_name(config)# ca subject-name myca ou=my_department, o=my_org, st=CA, c=US
```

Related Commands

show ca

ca verifycertdn

To verify the certificate's Distinguished Name (DN) and act as a subject name filter that is based on the *X.500_string*, use the **ca verifycertdn** command. To disable subject name filtering, use the **no** form of this command.

[**no**] **ca verifycertdn** *X.500_string*

Syntax Description

X.500_string	Character string that indicates the DN sent.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you enter the **ca verifycertdn** command and the subject name of the peer certificate matches the *X.500_string*, then it is filtered out and ISAKMP negotiation fails.

Examples

This example shows how to verify the certificate's DN:

```
fwsm/context_name(config)# ca verifycertdn woeruweoru
```

Related Commands

show ca

ca zeroize rsa

To delete all the RSA keys that were previously generated by the FWSM, use the **ca zeroize rsa** command.

ca zeroize rsa [*keypair_name*]

Syntax Description

keypair_name	(Optional) Name of the key pair.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **ca zeroize rsa** command deletes all the RSA keys that were previously generated by the FWSM. If you use this command, you must also perform two additional tasks as follows:

1. Use the **no ca identity** command to manually remove the FWSM's certificates from the configuration**.** This step deletes all the certificates that were issued by the CA.
2. Ask the CA administrator to revoke the FWSM's certificates at the CA. Supply the challenge password that you created when you originally obtained the FWSM's certificates using the **crypto ca enroll** command.

To save the RSA key pair, enter the **ca save all** command. To delete a specific RSA key pair, specify the name of the RSA key that you want to delete using the optional keyword *keypair_name* within the **ca zeroize rsa** command.

Note You may have more than one pair of RSA keys due to the Secure Shell (SSH). See the **ssh** command for more information.

Examples

This example shows how to delete the RSA keys:

```
fwsm/context_name(config)# ca zeroize rsa keys
```

Related Commands

show ca

capture

To enable packet capture capabilities for packet sniffing and network fault isolation, use the **capture** command. To disable packet capture capabilities, use the **no** form of this command.

capture *capture_name* [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**]

no capture *capture-name* [**access-list** *access_list_name*] [**circular-buffer**] [**interface** *interface_name*]

Syntax Description

capture_name	Name of the packet capture.
access-list *access_list_name*	(Optional) Selects packets based on IP or higher fields for a specific access list identification.
buffer *buf_size*	(Optional) Defines the buffer size used to store the packet in bytes.
ethernet-type *type*	(Optional) Selects an EtherType to exclude from capture.
interface *interface_name*	(Optional) Name of the interface on which to use packet capture.
packet-length *bytes*	(Optional) Sets the maximum number of bytes of each packet to store in the capture buffer.
circular-buffer	(Optional) Overwrites the buffer, starting from the beginning, when the buffer is full.

Defaults

The defaults are as follows:

- The **buffer** *size* is 512 KB.
- All theEtherTypes are accepted.
- All the IP packets are matched.
- The **packet-length** is 68 bytes.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Capturing packets is useful when troubleshooting connectivity problems or monitoring suspicious activity. The FWSM can track packet information for traffic that passes through the general-purpose processor, including management traffic and inspection engines. The FWSM cannot capture traffic that goes through the network processors (such as most through traffic). We recommend contacting technical support if you want to use the packet capture feature.

When selecting an EtherType to exclude from capture, an exception occurs with the 802.1Q or VLAN type. The 802.1Q tag is automatically skipped and the inner EtherType is used for matching. By default, all the EtherTypes are accepted.

Once the byte buffer is full, packet capture stops.

To enable packet capturing, attach the capture to an interface with the *interface* optional argument. Multiple interface statements attach the capture to multiple interfaces.

If you copy the buffer contents to a TFTP server in ASCII format, then you will see only the headers, not the details and hexadecimal dump of the packets. To see the details and hexadecimal dump, you need to transfer the buffer in PCAP format and then read it with TCPDUMP or Ethereal.

The **ethernet-type** and **access-list** optional keywords select the packets to store in the buffer. A packet must pass both the Ethernet and access list filters before the packet is stored in the capture buffer.

The **capture** *capture_name* **circular-buffer** command allows you to enable the capture buffer to overwrite itself, starting from the beginning, when the capture buffer is full.

Enter the **no capture** command with either the **access-list** or **interface** optional keyword unless you want to clear the capture itself. Entering **no capture** without optional keywords deletes the capture. If the **access-list** optional keyword is specified, the access list is removed from the capture and the capture is preserved. If the **interface** optional keyword is specified, the capture is detached from the specified interface and the capture is preserved.

Note The **capture** command is not saved to the configuration, and the **capture** command is not copied to the standby module during failover.

Use the **copy capture:** *capture_name* **tftp://server/***path* [**pcap**] command to copy capture information to a remote TFTP server.

Use the **https://***fwsm-ip-address***/capture/***capture_name*[**/pcap**] command to see the packet capture information with a web browser.

If you specify the **pcap** optional keyword, then a libpcap-format file is downloaded to the web browser and can be saved using the web browser. (A libcap file can be viewed with TCPDUMP or Ethereal.)

Examples

To enable packet capture, enter the following:

```
fwsm(config)# capture captest interface inside interface outside
```

On a web browser, the capture contents for a capture named “mycapture” can be viewed at the following location:

https://171.69.38.95/capture/mycapture/pcap

To download a libpcap file (used in web browsers such as Internet Explorer or Netscape Navigator) to a local machine, enter the following:

```
https://171.69.38.95/capture/http/pcap
```

This example shows that the traffic is captured from an outside host at 171.71.69.234 to an inside HTTP server:

```
fwsm/context_name(config)# access-list http permit tcp host 10.120.56.15 eq http host
171.71.69.234
fwsm/context_name(config)# access-list http permit tcp host 171.71.69.234 host
10.120.56.15 eq http
fwsm/context_name(config)# capture http access-list http packet-length 74 interface inside
```

This example shows how to capture ARP packets:

```
fwsm/context_name(config)# capture arp ethernet-type arp interface outside
```

Related Commands

clear capture
copy capture
show capture

cd

To change the current working directory to the one specified, use the **cd** command.

cd disk: *path*

Syntax Description

disk: *path*	Changes the current working directory.

Defaults

If you do not specify a directory, the directory is changed to the root of the disk.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to change to the config directory:

```
fwsm#(config)# cd disk:/config/
```

Related Commands

copy disk
copy flash
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir

changeto

To change the execution space in which commands are applied, use the **changeto** command.

changeto {**system** | **context** *name*}

Syntax Description

system	Changes the command execution space to system.
context	Changes the command execution space to context.
name	Execution space name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The name of the context is inserted in the command line prompt. The prompt changes only when you are working within a context. The prompt does not change when you change from single context mode to multiple context mode.

Examples

This example shows how to change to a context named “test1”:

```
fwsm(config)# changeto context test1
fwsm#/my_context(config)#
```

This example shows how to change from the context named “test1” back to the system context:

```
fwsm#/my_context(config)# changeto system
fwsm#(config)#
```

Related Commands

context

class

To create a class to which you can assign contexts and then enter the class submode, use the **class** command. Use the **no** form of this command to remove a class.

[**no**] **class** *name*

Syntax Description

name	Class name string of up to 20 characters.

Defaults

The default class is a special class to which all the unassigned contexts belong.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The class parameters determine the resource limitations for each class member.The class name is limited to 20 characters. The default class cannot be removed. Enter **default** for the *name* to change the limits for the default class. To remove a class, use the **no** form of this command. After you enter the **class** command, the FWSM enters the class subconfiguration mode. In this submode, you can enter the **limit-resource (class submode)** command.

By default, all the security contexts have access to most of the FWSM resources. However, if you find that one or more contexts use too many resources, and they cause other contexts to be denied connections, then you can configure resource management to limit the use of resources per context.

See the **limit-resource (class submode)** command for a list of resources. See also the **show resource types** command.

Note The FWSM does not limit the bandwidth per context. The switch/router containing the FWSM can limit the bandwidth per VLAN. Refer to the Catalyst 6500 series switch or Cisco 7600 series router documentation for more information.

Default Class

All the contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to default.

If a context belongs to another class, the other class settings always override the default class settings. However, if the other class has any settings that are not defined, then the member context uses the default class for those limits. For example, you create a class with a 2 percent limit for all the concurrent connections, but no other limits. All other limits are inherited from default. Conversely, if you create a class with a 2 percent limit for all the resources, the class uses no settings from default.

By default, the default class provides unlimited access to most resources for all the contexts. The following resources are limited by per context:

- Telnet—5
- SSH—5
- IPsec—5
- Bridge-table entries—65,535

All other contexts provide unlimited access.

Resource Members

To use the settings of a resource class, assign the context to the class. All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to the default. You can only assign a context to one resource class. The exception is that the limits that are undefined in the member class are inherited from the default class. A context could be a member of the default plus another class.

To assign a context to a class, enter the **member (context submode)** command.

Examples

This example shows how to create a class named “empire”:

```
fwsm(config)# class empire
fwsm#(config-class)# limit-resource all 50%
fwsm#(config-class)# limit-resource empire 50%
(config-class)# exit

fwsm(config)# show class
Class Name           Members    ID   Flags
default                All       1    0001
empire                   0       2    0000
```

This example shows how to change the default class parameters:

```
fwsm(config)# class default
fwsm#(config-class)# limit-resource all 10%
fwsm#(config-class)# limit-resource default 50%
fwsm#(config-class)# exit
```

Related Commands

config-url (context submode)
limit-resource (class submode)
show class
show context
show resource allocation
show resource types

clear

To remove configuration files and commands from the configuration or reset command values, use a form of the **clear** command.

clear *command*

Syntax Description

command	Item to remove or reset.

Defaults

The default setting depends on which **clear** command is used.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can use the **no** form of a command to change the configuration.

The **clear** commands can be used in modes with different security levels. The **clear** commands that can be used in less secure modes can also be used in more secure modes. However, if a **clear** command appears in a more secure mode, that command is not available in a less secure mode.

clear aaa

To enable, disable, or view TACACS+, RADIUS, or local user authentication, authorization, and accounting, use the **clear aaa** command.

clear aaa authentication | authorization | accounting

Syntax Description

authentication	Specifies AAA authentication.
authorization	Specifies AAA authorization.
accounting	Specifies AAA accounting.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove a defined server group:

```
fwsm/context_name(config)# clear aaa authentication
```

Related Commands

aaa-server
clear aaa accounting
clear aaa authentication
clear aaa authorization

clear aaa accounting

To clear the local, TACACS+, or RADIUS user account, use the **clear aaa accounting** command.

clear aaa accounting {**include** | **exclude**} *service interface_name source_ip source_mask* [*destination_ip destination_mask*] *server_tag*

include	Creates a new rule with the specified service to include.
exclude	Creates an exception to a previously stated rule by excluding the specified service from accounting.
service	Accounting service; valid values are **any**, **ftp**, **http**, **telnet**, or *protocol/port*.
interface_name	Interface name from which users require authentication.
source_ip	IP address of the source host or network of the hosts that you want to be authenticated or authorized.
source_mask	Network mask of the source IP.
destination_ip	(Optional) IP address of the hosts that you want to access the source IP address; **0** indicates all hosts.
destination_mask	(Optional) Network mask of the destination IP.
server_tag	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When specifying the *service*, use **any** to provide accounting for all the TCP services. To provide accounting for UDP services, use the *protocol/port* argument. For *protocol/port*, the TCP *protocol* appears as 6, the UDP protocol appears as 17, and so on, and the port is the TCP or UDP destination port. A port value of 0 (zero) indicates all the ports. For protocols other than TCP and UDP, the *port* is not applicable and should not be used. Enter **LOCAL** to use the local FWSM user authentication database.

Examples

This example shows how to clear the user account:

```
fwsm/context_name(config)# clear aaa accounting
```

Related Commands

aaa accounting

clear aaa authentication

To clear the local, TACACS+, or RADIUS user authentication, use the **clear aaa authentication** command.

clear aaa authentication {**include** | **exclude**} *authen_service interface_name source_ip source_mask* [*destination_ip destination_mask*] *server_tag*

Syntax Description

include	Creates a new rule with the specified service to include.
exclude	Creates an exception to a previously stated rule by excluding the specified service from accounting.
authen_service	Type of traffic to include or exclude from authentication based on the service optional keyword selected. See the "Usage Guidelines" section for valid values.
interface_name	Interface name from which users require authentication.
source_ip	IP address of the local host or network of the hosts that you want to be authenticated or authorized.
source_mask	Network mask of the local IP.
destination_ip	(Optional) IP address of the hosts that you want to access the local IP address; **0** indicates all hosts.
destination_mask	(Optional) Network mask of the destination IP.
server_tag	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Enter **LOCAL** to use the local FWSM user authentication database.

Examples

This example shows how to clear AAA authentication:

```
fwsm/context_name(config)# clear aaa authentication
```

Related Commands

aaa accounting

clear aaa authorization

To clear the local or TACACS+ user authentication, use the **clear aaa authorization** command.

clear aaa authorization {**include** | **exclude**} *authen_service interface_name source_ip source_mask* [*destination_ip destination_mask*] *server_tag*

Syntax Description

include	Creates a new rule with the specified service to include.
exclude	Creates an exception to a previously stated rule by excluding the specified service from accounting.
authen_service	Type of traffic to include or exclude from authentication based on the service optional keyword selected. See the "Usage Guidelines" section for valid values.
interface_name	Interface name from which users require authentication.
source_ip	IP address of the local host or network of the hosts that you want to be authenticated or authorized.
source_mask	Network mask of the local IP.
destination_ip	(Optional) IP address of the hosts that you want to access the local IP address; **0** indicates all hosts.
destination_mask	(Optional) Network mask of the destination IP.
server_tag	AAA server group tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **aaa authorization** command is supported for use with local and TACACS+ servers but not with RADIUS servers. Enter **LOCAL** to use the local FWSM user authentication database.

Examples

This example shows how to clear AAA authorization:

```
fwsm/context_name(config)# clear aaa authorization
```

Related Commands

aaa accounting
clear aaa authentication

clear aaa-server

To remove a defined server group, use the **clear aaa-server** command.

clear aaa-server [*tag*]

Syntax Description

tag	(Optional) AAA server group tag; enter **LOCAL** to use the local FWSM user authentication database.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove a defined server group:

```
fwsm/context_name(config)# clear aaa-server LOCAL
```

Related Commands

aaa-server

clear access-group

To remove access groups from all the interfaces, use the **clear access-group** command.

clear access-group

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the access groups:

```
fwsm/context_name(config)# clear access-group
```

Related Commands

access-group
show access-group

clear access-list

To remove an access list or clear an access-list counter, use the **clear access-list** command.

clear access-list [*id* [**counters**]]

Syntax Description

id	(Optional) Name or number of an access list.
counters	(Optional) Clears access-list counters.

Defaults

All the access lists are cleared.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When you enter the **clear access-list** command, all the **access-list** commands, including the **access-list deny-flow-max** command, are cleared if you do not specify an *id*. Also removed are commands that refer to an ACL, for example, the **access-group** command.

Examples

This example shows how to clear a specific access-list counter:

```
fwsm/context_name(config)# clear access-list 77 23 counters
```

This example shows how to clear all the access-list counters:

```
fwsm/context_name(config)# clear access-list inbound counters
```

Related Commands

access-list extended
show access-list

clear activation-key

To clear the FWSM activation key and revert the FWSM to the default feature set, use the **clear activation-key** command.

clear activation-key

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

In multiple security context mode, the default feature set allows two contexts.

Examples

This example shows how to clear an activation key:

```
fwsm(config)# clear activation-key
```

Related Commands

activation-key

clear alias

To remove all the **alias** commands from the configuration, use the **clear alias** command.

clear alias

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the **alias** commands from the configuration:

```
fwsm/context_name(config)# clear alias
```

Related Commands

alias

clear arp

To clear all the entries in the ARP cache table except for those you configure directly with the **arp** *interface_name ip mac* command, use the **clear arp** command.

clear arp [**timeout** | **statistics**]

Syntax Description

timeout	(Optional) Clears the ARP timeout.
statistics	(Optional) Clears the ARP statistics entries.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the ARP cache table entries:

```
fwsm/context_name(config)# clear arp
```

Related Commands

arp
show arp

clear arp-inspection

To clear the ARP inspection configuration, use the **clear arp-inspection** command.

clear arp-inspection

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Transparent

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the ARP inspection configuration:

```
fwsm/context_name(config)# clear arp-inspection
```

Related Commands

arp
arp-inspection
show arp

clear auth-prompt

To clear the AAA challenge text for HTTP, FTP, and Telnet access, use the **clear auth-prompt** command.

clear auth-prompt

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the AAA challenge text in the authorization prompt:

```
fwsm/context_name(config)# clear auth-prompt
```

Related Commands

auth-prompt
show auth-prompt

clear banner

To remove all the banners, use the **clear banner** command.

clear banner

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear banners:

```
fwsm/context_name(config)# clear banner
```

Usage Guidelines

banner
show banner

clear blocks

To remove all block information, use the **clear blocks** command.

clear blocks queue history

Syntax Description

queue	Specifies the block queue.
history	Specifies the blocks history.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear banners:

```
fwsm/context_name(config)# clear blocks
```

Usage Guidelines

show blocks

clear ca

To remove the Certificate Authority (CA) configuration, use the **clear ca** command.

clear ca

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the ca configuration:

```
fwsm/context_name(config)# clear ca
```

Usage Guidelines

ca configure
show ca

clear capture

To clear the capture buffer, use the **clear capture** *capture_name* command.

clear capture *capture_name*

Syntax Description

capture_name	Name of the packet capture.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The shortened form of the **clear capture** (for example, **cl cap** or **clear cap**) is not supported to prevent accidental destruction of all the packet captures.

Examples

This example shows how to clear the capture buffer for the capture buffer “orlando”:

```
fwsm/context_name(config)# clear capture orlando
```

Related Commands

capture
show capture

clear class

To remove all the classes and restore the default class to its default settings, use the **clear class** command.

clear class

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: config mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the classes:

```
fwsm(config)# clear class
```

Related Commands

class
show class

clear configure

To clear aspects of the running configuration, use the **clear configure** command.

clear configure {**primary** | **secondary** | **all**}

Syntax Description

primary	(Optional) Sets particular commands to their default values, removes interface names from all the commands in the configuration, and returns the commands to their default settings.
secondary	(Optional) Removes particular commands from the configuration and returns the commands to their default settings.
all	(Optional) Combines the entire running configuration and returns to the default settings.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear configure all** command resets a configuration to its default values. Use this command to create a template configuration or when you want to clear all the values.

Using the **clear config all** command in context mode clears the entire running configuration for a context, but it does not clear that context's configuration URL or delete the context. In addition, the parameters that are entered in the system configuration are not deleted.

Note If you enter the **clear configure** command in system mode, the system configuration and all context configurations are cleared.

The **clear configure primary** command resets the default values for the **interface**, **ip**, **mtu**, **nameif**, and **route** commands to their default values, removes interface names from all the commands in the configuration, and returns to the default settings.

The **clear configure secondary** command allows you to remove the **aaa-server**, **alias**, **access-list**, **apply**, **global**, **outbound**, **static**, **telnet**, and **url-server** commands from the configuration, and return to the default settings, but does not remove the **tftp-server** commands.

Use the **write erase** command to clear the startup configuration in the Flash partition.

Examples

This example shows how to clear the configuration in RAM:

```
fwsm/context_name(config)# clear configure all
```

Related Commands

configure
show configure
write

clear conn

To remove the connections from the system, use the **clear conn** command.

clear conn

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the connections from the system:

```
fwsm/context_name# clear conn
```

Related Commands

show conn

clear console-output

To remove the currently captured console output, use the **clear console-output** command.

clear console-output

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the currently configured console output:

```
fwsm/context_name# clear console-output
```

Related Commands

show console-output

clear context

To stop all contexts (including the admin context) from running and remove the context entries from the system configuration, use the **clear context** command.

clear context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear context** command clears all contexts, their configuration, and any context subcommands (member and config-url) for all contexts. The **clear context** command does not remove the RM class definitions.

Examples

This example show how to stop all the running contexts and remove the context entries from the system configuration:

```
fwsm(config)# clear context
```

Related Commands

context
show context

clear counters

To clear the protocol stack counters, use the **clear counters** command.

clear counters [**context** *context-name* | **top** *N* | **all** | **summary**] [**protocol** *protocol_name* [**:***counter_name*] | **detail**]

Syntax Description

context	(Optional) Specifies a context.
context-name	(Optional) Context name.
top *N*	(Optional) Displays the counter details for the specified location.
all	(Optional) Displays the filter details.
summary	(Optional) Displays a counter summary.
protocol	(Optional) Displays the counters for the specified protocol.
protocol_name	(Optional) Protocol by name.
:*counter_name*	(Optional) Counter by name.
detail	(Optional) Displays the counters in detail.

Defaults

clear counters summary detail

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the protocol stack counters:

```
fwsm(config)# clear counters
```

Related Commands

show counters

clear crashdump

To delete the crash information file from the Flash partition of the FWSM, use the **clear crashdump** command.

clear crashdump

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to delete the crash information file:

```
fwsm(config)# clear crashdump
```

Related Commands

crashdump force
show crashdump

clear crypto dynamic-map

To remove the **crypto dynamic-map** commands from the configuration, use the **clear crypto dynamic-map** command.

clear [**crypto**] **dynamic-map** [*dynamic-map-name*] [*dynamic-seq-num*]

Syntax Description

crypto	(Optional) Specifies crypto for the dynamic map.
dynamic-map-name	(Optional) Name of the dynamic crypto map set.
dynamic-seq-num	(Optional) Sequence number that corresponds to the dynamic crypto map entry.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **crypto** keyword is optional.

Examples

This example shows how to remove the **crypto dynamic-map** commands from the configuration:

```
fwsm/context_name(config)# clear crypto dynamic-map alarms 323
```

Related Commands

crypto dynamic-map
show crypto engine

clear crypto interface counters

To clear the crypto interface counters, use the **clear crypto interface counters** command.

clear crypto interface counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear crypto interface counters** command clears only the packet, payload byte, queue length, and moving average counters. It does not affect any actual packets that are queued.

Examples

This example shows how to clear the crypto interface counters:

```
fwsm#/context_name(config)# clear crypto interface counters
```

Related Commands

crypto map interface
show crypto interface

clear crypto ipsec sa

To delete IPSec security associations, use the **clear crypto ipsec sa** command.

clear [**crypto**] **ipsec sa** [**counters** | **entry** {*destination-address protocol spi*} | **map** *map-name* | **peer**]

Syntax Description

crypto	(Optional) Specifies the crypto configuration.
counters	(Optional) Clears the traffic counters that are maintained for each security association.
entry	(Optional) Deletes the IPSec security association with the specified address, protocol, and SPI.
destination-address	(Optional) IP address of the peer or the remote peer.
protocol	(Optional) Security associations by protocol; valid values are **ah** or **esp**.
spi	(Optional) Security Parameter Index (SPI) number that is used to identify a security association; valid values are from 256 to 4294967295 (a hexadecimal value of FFFF FFFF).
map *map-name*	(Optional) Deletes any IPSec security associations for the named crypto map set.
peer	(Optional) Deletes any IPSec security associations for the specified peer.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the security associations were established through the Internet Key Exchange (IKE), they are deleted. Future IPSec traffic requires new security associations. When IKE is used, the IPSec security associations are established only when needed.

If the security associations are manually established, the security associations are deleted.

If you enter the **clear** [**crypto**] **ipsec sa** command with no arguments, all the IPSec security associations are deleted.

If the security associations are manually established, the security associations are deleted and reinstalled. (When IKE is not used, the IPSec security associations are created as soon as the configuration is completed.)

If any of the previous commands cause a particular security association to be deleted, all the "sibling" security associations that were established during the same Internet Key Exchange (IKE) negotiation are deleted as well.

The **counters** optional keyword clears the traffic counters that are maintained for each security association; it does not clear the security association.

If you make configuration changes that affect security associations, these changes will not apply to existing security associations but to negotiations for subsequent security associations. You can use the **clear** [**crypto**] **ipsec sa** command to restart all the security associations so that they use the most current configuration settings. In the case of manually established security associations, if you make changes that affect security associations, you must use the **clear** [**crypto**] **ipsec sa** command before the changes take effect.

Note If you make significant changes to an IPSec configuration, such as access list or peers, the **clear** [**crypto**] **ipsec sa** command does not activate the new configuration. In such a case, you should rebind the crypto map to the interface with the **crypto map interface** command.

If the FWSM is processing active IPSec traffic, we recommend that you clear only the portion of the security association database that is affected by the changes to avoid causing active IPSec traffic to temporarily fail.

The **clear** [**crypto**] **ipsec sa** command clears only the IPSec security associations. To clear the IKE security associations, use the **clear** [**crypto**] **isakmp sa** command.

Examples

This example shows how to clear (and reinitialize, if appropriate) all the IPSec security associations at the FWSM:

```
fwsm/context_name(config)# clear crypto ipsec sa
```

This example shows how to clear (and reinitialize, if appropriate) the inbound and outbound IPSec security associations that are established for address 10.0.0.1 using the AH protocol with the SPI of 256:

```
fwsm/context_name(config)# clear crypto ipsec sa entry 10.0.0.1 AH 256
```

Related Commands

crypto ipsec security-association lifetime
crypto map interface
show crypto map

clear crypto isakamp sa

To remove the **isakamp policy** commands for IKE SAs from the configuration, use the **clear crypto isakamp sa** command.

clear crypto isakamp sa

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the **isakamp policy** commands from the configuration:

```
fwsm/context_name(config)# clear isakamp sa
```

Related Commands

isakmp
isakmp policy
show isakmp
show isakmp policy

clear dhcpd

To clear all of the DHCP server commands, binding, and statistics information, use the **clear dhcp** command.

clear dhcpd [**binding** | **statistics**]

Syntax Description

binding	(Optional) Clears all the client address bindings.
statistics	(Optional) Clears statistical information, such as the address pool, number of bindings, malformed messages, sent messages, and received messages.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear dhcpd** command clears all of the **dhcpd** commands, binding, and statistics information. The **clear dhcp statistics** command clears the **show dhcp statistics** counters.

Examples

This example shows how to clear the **dhcpd** commands:

```
fwsm/context_name(config)# clear dhcpd statistics
```

Related Commands

dhcpd
dhcprelay
show dhcpd
show dhcprelay

clear dhcprelay

To clear the DHCP-relay configuration commands, use the **clear dhcprelay** command.

clear dhcprelay [**statistics**]

Syntax Description

statistics	(Optional) Clears the DHCP relay statistical counters.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear dhcprelay** command clears all DHCP relay configurations. The **clear dhcprelay statistics** command clears the **show dhcprelay statistics** counters.

Examples

This example shows how to clear all DHCP relay configurations:

```
fwsm/context_name(config)# clear dhcprelay statistics
```

Related Commands

dhcpd
dhcprelay
show dhcpd
show dhcprelay

clear dispatch stats

To clear dispatch layer statistics, use the **clear dispatch stats** command.

clear dispatch stats [**funcid** | **all**]

Syntax Description

funcid	(Optional) Specifies the dispatch layer statistics function ID.
all	(Optional) Specifies all dispatch layer statistics.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all of the dispatch layer statistics:

```
fwsm(config)# clear dispatch stats all
```

Related Commands

show dispatch stats
show dispatch table

clear dynamic-map

To delete a dynamic crypto map entry, use the **clear dynamic-map** command.

clear [**crypto**] **dynamic-map** [*dynamic-map-name*] [*dynamic-seq-num*]

Syntax Description

crypto	(Optional) Specifies the crypto configuration
dynamic-map-name	(Optional) Map name.
dynamic-seq-num	(Optional) Map sequence number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove a dynamic map entry:

```
fwsm/context_name(config)# clear dynamic-map
```

Related Commands

crypto dynamic-map
dynamic-map

clear established

To remove all established commands, use the **clear established** command.

clear established

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To remove an established connection created by the **established** command, enter the **clear xlate** command.

Examples

This example shows how to remove established commands:

```
fwsm/context_name(config)# clear established
```

Related Commands

established
show established

clear failover

To remove all failover configurations, use the **clear failover** command.

clear failover

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the failover configuration:

```
fwsm(config)# clear failover
```

Related Commands

failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
failover reset
show failover
write standby

clear filter

To remove all **filter** commands from the configuration, use the **clear filter** command

clear filter

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all **filter** commands:

```
fwsm/context_name(config)# clear filter
```

Related Commands

filter ftp
filter https
filter url

clear firewall

To set the firewall mode to the default setting, use the **clear firewall** command

clear firewall

Syntax Description

This command has no arguments or keywords.

Defaults

The default firewall mode is routed.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to set the firewall mode to routed:

```
fwsm/context_name(config)# clear firewall
```

Related Commands

firewall
show firewall

clear fixup

To reset the fixup configuration, use the **clear fixup** command.

clear fixup

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear fixup** command does not remove the default **fixup protocol** commands.

Examples

This example shows how to reset the fixup configuration:

```
fwsm/context_name(config)# clear fixup
```

Related Commands

fixup protocol
show fixup

clear flashfs

To clear the file system part of the Flash partition in the FWSM, use the **clear flashfs** command.

clear flashfs

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear flashfs** command clears the file system part of the Flash partition in the FWSM.

The **clear flashfs** command does not affect the configuration that is stored in the Flash partition.

Examples

This example shows how to clear the file system part of the Flash partition on the FWSM:

```
fwsm# clear flashfs
```

Related Commands

clear flashfs
no flashfs
show flashfs

clear floodguard

To disable flood guard, use the **clear floodguard** command.

clear floodguard

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable flood guard:

```
fwsm/context_name(config)# clear floodguard
```

Related Commands

floodguard
show floodguard

clear fragment

To reset the fragment databases and defaults, use the **clear fragment** command.

clear fragment

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear fragment** command resets the fragment databases. Specifically, all fragments awaiting reassembly are discarded. In addition, the size is reset to 200, the chain limit is reset to 24, and the timeout is reset to 5 seconds.

All fragments currently waiting for reassembly are discarded and the **size**, **chain**, and **timeout** optional keywords are reset to their default values.

The **sysopt security fragguard** and **fragguard** commands have been replaced by the **fragment** command.

Examples

This example shows how to reset the fragment database and defaults:

```
fwsm/context_name(config)# clear fragment
```

Related Commands

fragment
show fragment

clear ftp

To set the FTP mode to the default setting, use the **clear ftp** command.

clear ftp

Syntax Description

This command has no arguments or keywords.

Defaults

The default FTP mode is passive.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

Tis example shows how to set the FTP mode to passive:

```
fwsm(config)# clear ftp
```

Related Commands

ftp mode
show ftp

clear gc

To remove the garbage collection process statistics, use the **clear gc** command.

clear gc

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the garbage collection process statistics:

```
fwsm# clear gc
```

Related Commands

show gc

clear global

To remove the **global** commands from the configuration, use the **clear global** command.

clear global

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Transparent

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the **global** commands from the configuration:

```
fwsm/context_name(config)# clear global
```

Related Commands

global
show global

clear hostname

To clear the host name in the FWSM command line prompt, use the **clear hostname** command.

clear hostname

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to change a host name:

```
fwsm(config)# clear hostname
fwsm(config)#
```

Related Commands

hostname
show hostname

clear http

To remove all HTTP hosts and disable the server, use the **clear http** command.

clear http

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all HTTP hosts and disable the HTTP servers:

```
fwsm/context_name(config)# clear http
```

Related Commands

http
show http

clear icmp

To remove the access for ICMP traffic that terminates at an interface, use the **clear icmp** command.

clear icmp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear icmp** command clears the ICMP entries.

Examples

This command shows how to remove the access for ICMP traffic:

```
fwsm/context_name(config)# clear icmp
```

Related Commands

icmp
show http

clear interface stats

To clear the interface statistics, use the **clear interface stats** command.

clear interface [*interface*] **stats**

Syntax Description

interface-id	(Optional) Interface identification name or number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear interface** command clears all the interface statistics. This command does not shut down all the system interfaces. The **clear interface** command also clears the packet drop count of Unicast RPF for all interfaces.

Examples

This command shows how to clear the statistics for the inside interface:

```
fwsm/context_name(config)# clear interface inside stats
```

Related Commands

interface
show interface

clear ip address

To clear all the IP addresses, use the **clear ip address** command.

clear ip address

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

After changing an **ip address** command, use the **clear xlate** command.

Examples

This example shows how to clear all the interface IP addresses and stop all traffic through the FWSM module:

```
fwsm/context_name(config)# clear ip address
```

Related Commands

clear ip verify reverse-path
ip address
ip prefix-list
ip verify reverse-path
show ip address
show ip verify

clear ip ospf

To clear information about the IP OSPF, use the **clear ospf** command.

clear ip ospf [*pid*] {**process | counters | neighbor** [**neighbor-intf**] [**neighbr-id**]}

Syntax Description

pid	(Optional) Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
process	Clears the OSPF routing process ID.
counters	Clears the OSPF counters.
neighbor	Clears the OSPF neighbor.
neighbor-intf	(Optional) Clears the OSPF interface router designation.
neighbr-id	(Optional) Clears the OSPF neighbor router ID.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command does not remove any part of the configuration. To remove the OSPF configuration, use the **no** form of the **router ospf** or **routing interface** command.

Examples

This example shows how to clear the OSPF IP parameters:

```
fwsm/context_name(config)# clear ip ospf
```

Related Commands

routing interface
show ip ospf

clear ip verify reverse-path

To remove the **ip verify reverse-path** commands from the configuration, use the **clear ip verify reverse-path** command.

clear ip verify reverse-path [**interface** *int_name*] [**statistics**]

Syntax Description

interface *int_name*	Removes the **ip verify reverse-path** command configuration from the configuration.
statistics	(Optional) Removes the statistical information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear ip verify** command allows you to remove the **ip verify** commands from the configuration. Unicast reverse path forwarding (RPF) is a unidirectional input function that screens inbound packets arriving on an interface. The outbound packets are not screened.

Examples

This example shows how to remove the **ip verify reverse-path** commands from the configuration:

```
fwsm/context_name(config)# clear ip verify reverse-path
```

Related Commands

clear ip address
ip address
ip prefix-list
ip verify reverse-path
show ip address
show ip verify

clear local-host

To clear the information that is displayed for the local hosts, use the **clear local-host** command.

Note Clearing the network state of a local host stops all connections and xlates that are associated with the local hosts.

clear local-host [*ip_address*]

Syntax Description

ip_address	(Optional) Local host IP address.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use the *ip_address* option to limit the display to a single host.

On the FWSM, the cleared hosts are released from the license limit. You can see the number of hosts that are counted toward the license limit by entering the **show local-host** command.

Examples

This example shows how the **clear local-host** command clears the information about the local hosts:

```
fwsm/context_name(config)# clear local-host 10.1.1.15
fwsm/context_name(config)# show local-host 10.1.1.15
```

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Related Commands

show local-host

clear logging rate-limit

To reset the disallowed messages to the original set, use the **clear logging rate-limit** command.

clear logging rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to reset the disallowed messages:

```
fwsm/context_name(config)# clear logging rate-limit
```

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Related Commands

show logging rate-limit

clear mac-address-table

To remove the interface name entries from the bridge table, use the **clear mac-address-table** command.

clear mac-address-table *interface_name*

Syntax Description

interface_name	Specifies the interface name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Transparent

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the interface name entries from the bridge table:

```
fwsm/context_name(config)# clear mac-address-table my_context
```

Related Commands

mac-address-table aging-time
mac-address-table static
show mac-address-table

clear mac-learn

To stop MAC learning, use the **clear mac-learn** command.

clear mac-learn

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: Transparent

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to stop MAC learning:

```
fwsm(config)# clear mac-learn
```

Related Commands

show mac-learn

clear mgcp

To remove the Media Gateway Command Protocol (MGCP) configuration and reset the command queue limit to the default of 200, use the **clear mgcp** command.

clear mgcp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the MGCP configuration and reset the command queue:

```
fwsm/context_name(config)# clear mgcp
```

Related Commands

mgcp
show mgcp

clear monitor-interface

To remove the interface-monitor configuration for failover, use the **clear monitor-interface** command.

clear monitor-interface

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the interface monitor configuration:

```
fwsm/context_name(config)# clear monitor-interface
```

Related Commands

failover
monitor-interface
show monitor-interface

clear mp-passwd

To remove the maintenance partition password and reset to the default password, use the **clear mp-passwd** command.

clear mp-passwd

Syntax Description

This command has no arguments or keywords.

Defaults

The default password is “cisco.”

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the maintenance partition password:

```
fwsm(config)# clear mp-passwd
```

Related Commands

upgrade-mp

clear nat

To remove the NAT configuration, use the **clear nat** command.

clear nat

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines

Note In transparent firewall mode, only NAT id 0 is valid.

Examples

This example shows how to remove the NAT configuration:

```
fwsm/context_name(config)# clear nat
```

Related Commands

clear nat
nat
show nat

clear name

To clear the list of names from the FWSM configuration, use the **clear name** command.

clear name

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the name list from the FWSM:

```
fwsm/context_name(config)# clear name
```

Related Commands

clear names
name
names
show name
show names

clear names

To disable the use of the **name** commands, use the **clear names** command.

clear names

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable the use of the names:

```
fwsm/context_name(config)# clear names
```

Related Commands

clear name
name
names
show name
show names

clear object-group

To remove all the **object group** commands from the configuration, use the **clear object-group** command.

clear object-group [{**protocol** | **service** | **icmp-type** | **network**}] [*obj_grp_id*]

Syntax Description

protocol	(Optional) Clears a protocol group.
service	(Optional) Clears a service group.
icmp-type	(Optional) Clears an ICMP group.
network	(Optional) Clears a network group.
obj_grp_id	(Optional) Name of a previously defined object group.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the **object-group** commands from the configuration:

```
fwsm/context_name(config)# clear object-group
```

Related Commands

object-group
show object-group

clear pager

To restore the **pager** command default settings, use the **clear pager** command.

clear pager

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: unprivileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to restore the **pager** command default settings:

```
fwsm> clear pager
```

Related Commands

pager
show pager

clear password

To reset the password to “cisco,” use the **clear password** command.

clear {**password** | **passwd**}

Syntax Description

password	Specifies that you are clearing the password.
passwd	Specifies that you are clearing the password

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: config mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to reset the password to “cisco”:

```
fwsm(config)# clear password
```

Related Commands

password/passwd
show password/passwd

clear pdm

To remove all the FWSM Device Manager locations, disable logging, and clear the PDM buffer, use the **clear pdm** command.

clear pdm [**location** | **group** | **logging**]

Syntax Description

location	(Optional) Specifies the PDM location.
group	(Optional) Specifies the PDM group.
logging	(Optional) Specifies the logging messages and level.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear pdm**, **pdm group**, **pdm history**, **pdm location**, and **pdm logging** commands may appear in the configuration, but they are designed to work as internal PDM-to-FWSM commands accessible only to the PDM buffer.

Examples

This example shows how to remove all the FWSM Device Manager locations, disable logging, and clear the PDM buffer:

```
fwsm(config)# clear pdm
```

Related Commands

pdm
show pdm

clear privilege

To remove the configuration or display privilege levels for the commands, use the **clear privilege** command.

clear privilege

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the configuration or display privilege levels for the commands:

```
fwsm(config)# clear privilege
```

Related Commands

privilege
show privilege

clear resource usage

To set the peak counter to the value of the current counter and clear the denied counter, use the **clear resource usage** command.

clear resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**} | **detail**]

Syntax Description

context	(Optional) Specifies the context.
context_name	(Optional) Name of the context.
top *n*	(Optional) Specifies a number of resources.
all	(Optional) Specifies all resources.
summary	(Optional) Specifies a summary of resources.
system	(Optional) Specifies the system resources.
resource	(Optional) Specifies a specific resource.
rate	(Optional) Specifies a resource rate.
resource_name	(Optional) Resource name.
all	(Optional) Specifies all resources.
detail	(Optional) Specifies the details.

Defaults

All configurable resources.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear resource usage** command operates on the resources specified in the command. If no resource type is specified, the command uses the default for all resources. If the resource type detail is specified, all resource types are cleared.

Examples

This example show how to remove the list of system resources that were used:

```
fwsm(config)# clear resource usage
```

Related Commands

show resource allocation
show resource types
show resource usage

clear rip

To remove the Routing Information Protocol (RIP) settings, use the **clear rip** command.

clear rip

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the RIP settings:

```
fwsm(config)# clear rip
```

Related Commands

rip
show rip

clear route

To remove the **route** commands from the configuration that does not contain the **connect** keyword, use the **clear route** command.

clear route [*interface_name ip_address* [*netmask gateway_ip*]]

Syntax Description

interface_name	(Optional) Internal or external network interface name.
ip_address	(Optional) Internal or external network IP address.
netmask	(Optional) Specifies a network mask to apply to the *ip_address*.
gateway_ip	(Optional) Specifies the IP address of the gateway router (the next hop address for this route).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use **0.0.0.0** to specify a default route. You can abbreviate the 0.0.0.0 IP address as **0** and the 0.0.0.0 *netmask* as **0**.

Examples

This example shows how to remove the **route** commands from the configuration that does not contain the **connect** keyword:

```
fwsm(config)# clear route
```

Related Commands

route
show route

clear route-map

To remove the conditions for redistributing the routes from one routing protocol into another routing protocol, use the **clear route-map** command.

clear route-map *map_tag* [**permit** | **deny**] [*seq_num*]

Syntax Description

map_tag	Text for the route map tag. Defines a meaningful name for the route map up to 58 characters in length.
permit	(Optional) Specifies that if the match criteria are met for this route map, the route is redistributed as controlled by the set actions.
deny	(Optional) Specifies that if the match criteria are met for the route map, the route is not redistributed.
seq_num	(Optional) Route map sequence number; valid values are from 0 to 65535.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the match criteria are not met, and the **permit** keyword is specified, 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

This example shows how to remove the conditions of redistributing routes from one routing protocol into another routing protocol:

```
fwsm(config)# clear route-map 77 permit
```

Related Commands

route
route-map
show route

clear routing

To reset the interface-specific routing configuration to its defaults and remove the interface-specific routing configuration, use the **clear routing** command.

clear routing

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command does not remove any OSPF data structures that have been defined.

Examples

This example shows how to reset the interface-specific routing configuration to its default settings and remove the interface-specific routing configuration:

```
fwsm(config)# clear routing
```

Related Commands

route
route-map
show route

clear rpc-server

To clear the remote processor call (RPC) services from the FWSM, use the **clear rpc-server** command.

clear rpc-server [**active**]

Syntax Description

active	(Optional) Identifies the RPC services that are currently active on the FWSM.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **rpc-server** command displays the configured **router ospf** subcommands.

Note If the highest-level IP address on the FWSM is a private address, this address is sent in hello packets and database definitions (DBDs). To prevent this action, set the **router-id** *ip_address* to a global address.

Examples

This example shows how to clear the RPC services from the FWSM:

```
fwsm(config)# clear rpc-server active
```

Related Commands

rpc-server
show rpc-server

clear same-security-traffic

To disable the same-security interface communication, use the **clear same-security-traffic** command.

clear same-security-traffic

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable the same-security interface communication:

```
fwsm(config)# clear same-security-traffic
```

Related Commands

same-security-traffic
show routing

clear service

To remove the **service** commands from the configuration, use the **clear service** command.

clear service

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the **service** commands from the configuration:

```
fwsm/context_name(config)# clear service
```

Related Commands

service
show service

clear shun

To disable all the shuns that are currently enabled and clear the shun statistics, use the **clear shun** command.

clear shun [*statistics*]

Syntax Description

statistics	(Optional) Interface counters only.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable all the shuns that are currently enabled and clear the shun statistics:

```
fwsm/context_name(config)# clear shun
```

Related Commands

show shun
shun

clear snmp-server

To disable the Simple Network Management Protocol (SNMP) server, use the **clear snmp-server** command.

clear snmp-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable the SNMP server:

```
fwsm/context_name(config)# clear snmp-server
```

Related Commands

show snmp-server
snmp-server

clear ssh

To remove all the **ssh** commands from the configuration, use the **clear ssh** command.

clear ssh

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the **ssh** commands from the configuration:

```
fwsm/context_name(config)# clear ssh
```

Related Commands

show ssh
ssh

clear static

To remove all the **static** commands from the configuration, use the **clear static** command.

clear static

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Examples

This example shows how to remove all the **static** commands from the configuration:

```
fwsm/context_name(config)# clear static
```

Related Commands

show ssh
static

clear sysopt

To remove all the **sysopt** commands from the configuration, use the **clear sysopt** command.

clear sysopt

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the **sysopt** commands from the configuration:

```
fwsm/context_name(config)# clear sysopt
```

Related Commands

show sysopt
sysopt

clear tacacs-server

To remove all the **tacacs-server** commands from the configuration, use the **clear tacacs-server** command.

clear tacacs-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove all the **tacacs-server** commands from the configuration:

```
fwsm/context_name(config)# clear tacacs-server
```

Related Commands

aaa-server
telnet

clear telnet

To remove the Telnet connection and the idle timeout from the configuration, use the **clear telnet** command.

clear telnet [*ip_address* [*netmask*] [*interface_name*]]

Syntax Description

ip_address	(Optional) IP address of a host or network that can access the FWSM Telnet console.
netmask	(Optional) Bit mask of *ip_address*.
interface_name	(Optional) Unsecure interface name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To limit access to a single IP address, use 255 in each octet; for example, 255.255.255.255. If you do not specify *netmask*, it defaults to 255.255.255.255 regardless of the class of *source_ip*. Do not use the subnetwork mask of the internal network. The *netmask* is only a bit mask for the IP address in *ip_address*.

If IPSec is operating, you can specify an unsecure interface name, typically, the outside interface. At a minimum, you must configure the **crypto map** command to specify an interface name with the **telnet** command.

If you do not specify an interface name, the address is assumed to be on an internal interface. The FWSM automatically verifies the IP address against the IP addresses that are specified by the **ip address** commands to ensure that the address that you specify is on an internal interface. If an interface name is specified, the FWSM checks only the host against the interface that you specify.

Up to 16 hosts or networks are allowed access to the FWSM console with Telnet; 5 hosts or networks are allowed access to the console at the same time. Use the **no telnet** or **clear telnet** commands to remove Telnet access from a previously set IP address. Use the **telnet timeout** command to set the maximum time that a console Telnet session can be idle before being logged off by the FWSM. The **clear telnet** command does not affect the **telnet timeout** command duration. You cannot use the **no telnet** command with the **telnet timeout** command.

Examples

This example shows how to remove the Telnet connection and the idle timeout from the FWSM configuration:

```
fwsm/context_name(config)# clear telnet
```

Related Commands

show telnet
telnet

clear terminal

To remove the console terminal line parameter settings, use the **clear terminal** command.

clear terminal

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the console terminal line parameter settings from the FWSM configuration:

```
fwsm/context_name(config)# clear terminal
```

Related Commands

show telnet
terminal

clear tftp-server

To remove the Trivial File Transfer Protocol (TFTP) server address and directory from the configuration, use the **clear tftp-server** command.

clear tftp-server [[*interface_name*] *ip_address path*]

Syntax Description

interface_name	(Optional) Interface name on which the TFTP server resides.
ip_address	(Optional) IP address or network of the TFTP server.
path	(Optional) Path and filename of the configuration file.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If not specified, an internal interface is assumed. If you specify the outside interface, a warning message informs you that the outside interface is unsecure. The contents of the path are passed directly to the server without interpretation or checking. The format for the path differs by the type of operating system on the server. The configuration file must exist on the TFTP server. Many TFTP servers require the configuration file to be world-writable to write to it and world-readable to read from it.

Examples

This example shows how to remove the TFTP server address and directory from the configuration:

```
fwsm/context_name(config)# clear tftp-server
```

Related Commands

show tftp-server
tftp-server

clear timeout

To remove the maximum idle time durations from the configuration, use the **clear timeout** command.

clear timeout

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the maximum idle time durations from the configuration:

```
fwsm/context_name(config)# clear timeout
```

Related Commands

show timeout
timeout

clear uauth

To delete all the authorization caches for a user, use the **clear uauth** command.

clear uauth [*username*]

Syntax Description

username	(Optional) Username to enter, to clear, or view user authentication information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear uauth** command deletes one user or all the users' AAA authorization and authentication caches, which forces the user or users to reauthenticate the next time that they create a connection.

This command is used with the **timeout** command.

Each user host IP address has an authorization cache attached to it. If you attempt to access a service that has been cached from the correct host, the FWSM considers it preauthorized and immediately proxies the connection. Once you are authorized to access a website, the authorization server is not contacted for each image as it is loaded (assuming the images come from the same IP address). This process significantly increases performance and reduces the load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization purposes, the IP address to which the username is bound, and whether the user is authenticated only or has cached services.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. For this reason, a uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see to the **aaa** commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all the authorization caches for all the users, which will cause them to have to reauthenticate the next time that they create a connection.

Examples

This example shows how to cause the user "Pat" to reauthenticate:

```
fwsm(config)# clear uauth pat
```

Related Commands

aaa authorization
show uauth
timeout

clear url-block

To clear the pending URL block buffer and long URL support usage counters, use the **clear url-block** command.

clear url-block

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The “Current number of packets held (global)” counter is not cleared.

Examples

This example shows how to clear the pending URL block buffer and long URL support usage counters:

```
fwsm/context_name(config)# clear url-block
```

Related Commands

show url-block
url-block

clear url-cache

To disable URL caching, use the **clear url-cache** command.

clear url-cache

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to disable URL caching:

```
fwsm/context_name(config)# clear url-cache
```

Related Commands

show url-cache stat
url-cache

clear url-server

To remove the URL filter server from the configuration, use the **clear url-server** command.

clear url-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the URL filter server from the configuration:

```
fwsm(config)# clear url-server
```

Related Commands

show url-server
url-server

clear username

To remove usernames from the user authentication local database, use the **clear username** command.

clear username

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove usernames from the user authentication local database:

```
fwsm(config)# clear username
```

Related Commands

show username
username

clear virtual

To remove the authentication virtual server from the configuration, use the **clear virtual** command.

clear virtual

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to remove the authentication virtual server from the configuration:

```
fwsm/context_name(config)# clear virtual
```

Related Commands

show virtual
virtual

clear vpngroup

To clear the Easy VPN Remote configuration and security policy that is stored in the Flash partition, use the **clear vpngroup** command.

clear vpngroup

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to clear the Easy VPN Remote configuration and security policy that is stored in the Flash partition:

```
fwsm/context_name(config)# clear vpngroup
```

Related Commands

show vpngroup
vpngroup

clear xlate

To clear the current translation and connection slot information, use the **clear xlate** command.

clear xlate [**global** | **local** *ip1*[**-***ip2*] [**netmask** *mask*]] {**gport** | **lport** *port1* [**-***port2*]] [**interface** *if1*[**,***ifn*]] [**state** *static* [**,portmap**] [**,norandomseq**] [**,identity**]] [**debug**] [**count**]

Syntax Description

global | **local** *ip1* **-***ip2* **netmask** *mask*	(Optional) Clears the active translations by global IP address or local IP address using the network mask to qualify the IP addresses.
interface *if1* **,***if2* **,***ifn*	(Optional) Clears the active translations by interface.
gport | **lport** *port* **-***port2*	(Optional) Clears the active translations by local and global port specifications. See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names.
interface	(Optional) Displays the active translations by interface.
if1 **,***if2*	(Optional) Specifies the interface.
state *static*	(Optional) Clears the active translations by state; valid values are static translation (**static**), **dump** (cleanup), PAT **global** (**portmap**), **nat** or **static** translation with the **norandomseq** setting (**norandomseq**), or the use of the **nat 0**, or identity feature (**identity**).
,portmap	(Optional) Specifies the port map.
norandomseq	(Optional) Specifies no random sequence.
,identity	(Optional) Specifies the identity.
debug	(Optional) Specifies debugging.
count	(Optional) Specifies the count.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear xlate** command clears the contents of the translation slots. ("xlate" refers to the translation slot.) Always use the **clear xlate** command because translation slots can persist after adding, changing, or removing the **aaa-server**, **access-list**, **alias**, **global**, **nat**, **route**, or **static** commands in the configuration.

Examples

This example shows how to clear the current translation and connection slot information:

```
fwsm/context_name(config)# clear xlate global
```

Related Commands

show conn
show uauth
show xlate
timeout

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** subcommand. To disable RFC 1583 compatibility, use the **no** form of this command.

[**no**] **compatible rfc1583**

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- OSPF routing is disabled on the FWSM.
- OSPF routing through the FWSM is compatible with RFC 1583.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The Open Shortest Path First (OSPF) protocol is used instead of the Routing Information Protocol (RIP). Do not attempt to configure the FWSM for both OSPF and RIP simultaneously.

The **compatible rfc1583** command is a subcommand of the **router ospf** command. The **router ospf** command is the global configuration command for OSPF routing processes running on the FWSM. The **compatible rfc1583** command is the main command for all of the OSPF configuration commands.

The **show ip ospf** command displays the configured **router ospf** subcommands.

The **compatible rfc1583** subcommand is displayed in the configuration only if it is disabled by the **no compatible rfc1583** subcommand. It displays as “no compatible rfc1583.”

Examples

This example shows how to restore the method that is used to calculate the summary route costs per RFC 1583:

```
fwsm#/context_name(config)# compatible rfc1583
```

Related Commands

router ospf
show ip ospf

configure

To configure from the terminal, Flash partition, or the network, use the **configure** command. To remove configurations, use the **clear configure** command.

configure [**terminal** | **memory**]

configure net [[*tftp_ip*]**:**[*filename*]]

Syntax Description

terminal	(Optional) Configures from the terminal connection.
memory	(Optional) Configures memory.
net	Loads the configuration from a TFTP server and the specified path.
tftp_ip	(Optional) IP address or name of the server from which to merge in a new configuration.
filename	(Optional) Filename that you specify to qualify the location of the configuration file on the TFTP server named in *server_ip*.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can configure from the terminal, Flash partition, or the network. The new configuration merges with the active configuration.

You must be in privileged mode to use the **configuration** commands, except for the **configure terminal** (**config t**) command which allows you to start configuration mode from the privileged mode. You can exit configuration mode with the **quit** command. Use the **write memory** command to store the changes in the Flash partition, or use the **write floppy** command to store the configuration on disk.

Each command from the Flash partition (with **configure memory**) and TFTP transfer (with **configure net**) is read and evaluated as follows:

- If the command in the Flash partition or on the disk is identical to an existing command in the current configuration, it is ignored.
- If the command in the Flash partition or on the disk is an additional instance of an existing command, then both commands appear in the current configuration.

- If the command redefines an existing command, the command on the disk or Flash partition overwrites the command in the current configuration in RAM. For example, if you have the **hostname ram** command in the current configuration and the **hostname floppy** command on the disk, the command in the configuration becomes **hostname floppy** and the command line prompt changes to match the new host name when that command is read from disk.

If you set a *filename* with the **tftp-server** command, do not specify it in the **configure** command; instead use a colon (**:**) without a filename.

The guidelines for the **configure net** command are as follows:

- The **configure net** command allows you to merge the current running configuration with a TFTP configuration stored at the IP address that you specify and from the file that you name. If you specify both the IP address and pathname in the **tftp-server** command, you can specify *server_ip* **:***filename* as a colon (**:**). For example, you can specify **configure net :**.
- Use the **write net** command to store the configuration in the file.
- If you have an existing FWSM configuration on a TFTP server and store a shorter configuration with the same filename on the TFTP server, some TFTP servers will leave some of the original configuration after the first ":end" mark. This situation does not affect the FWSM because the **configure net** command stops reading when it reaches the first ":end" mark. This situation does not occur if you are using Cisco TFTP Server version 1.1 for Windows NT.

Note Many TFTP servers require the configuration file to be world-readable to be accessible.

The **configure memory** command allows you to merge the configuration in the Flash partition into the current configuration in RAM.

Examples

This example shows how to configure the FWSM using a configuration retrieved with TFTP:

```
fwsm/context_name(config)# configure net 10.1.1.1:/tftp/config/fwsmconfig
```

The FWSM configuration file is stored on the TFTP server at 10.1.1.1 in the tftp/config folder.

This example shows how to configure the FWSM from the configuration that is stored in the Flash partition:

```
fwsm/context_name(config)# configure memory
```

Access privileged mode with the **enable** command and configuration mode with the **configure terminal** command. View the current configuration with the **write terminal** command and save the configuration to the Flash partition using the **write memory** command.

```
fwsm> enable
password:
fwsm# configure terminal
fwsm(config)# write terminal
:  Saved
[… current configuration …]
:  End
fwsm(config)# write memory
```

When you enter the **configure factory-default** command on a platform other than the FWSM, the FWSM displays a "not supported" error message. On the FWSM, this message is displayed:

```
fwsm(config)# configure factory default
'config factory-default' is not supported on FWSM
```

Related Commands

show configure

config-url (context submode)

To set the URL from which the FWSM downloads the context file, use the **config-url** command. To return to the default setting, use the **no** form of this command.

[**no**] **config-url** *url*

Syntax Description

url	URL from which the FWSM downloads the context file (text format).

Defaults

The default *number* is 0, which means the console will not time out.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Enter the **allocate-interface (context submode)** command(s) before you enter the **config-url** command. The FWSM must assign VLAN interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**nameif**, **nat**, **global**...). If you enter the **config-url** command first, the FWSM loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

When you add a context URL, the FWSM immediately loads the context so that it is running. The URL syntax is as follows:

```
disk://[<path>/]<filename>
ftp://<server>/[<path>/]<filename>
tftp://<server>/[<path>/]<filename>
http://<server>/[<path>/]<filename>
https://<server>/[<path>/]<filename>
```

You can download the context from a TFTP or FTP server, HTTP or HTTPS server, or from the local disk (called **disk**). The disk is a 64-MB partition of the Flash partition that uses a navigatible file system (and the associated commands). The disk partition is used only for context storage. The startup configuration (which in multiple security context mode is the system configuration) and software image reside in the Flash partition (called Flash), which uses the FWSM Flash file system.

The URL must be accessible from the admin context. The admin context file must be stored on the disk.

Although the filename does not require a file extension, you should use .cfg.

If the FWSM cannot retrieve the context configuration file because the server is unavailable, or the file does not exist, the FWSM creates a blank context that is ready for you to configure with the command-line interface (CLI).

To change a context's URL, you can enter the **config-url** command again with a new URL. However, the new configuration does not overwrite the existing one; instead, the FWSM merges the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used.

Examples

This example shows how to set the console timeout to 15 minutes:

```
fwsm(config)# context cisco
fwsm/context_name(config)# allocate-interface vlan100 int0
fwsm/context_name(config)# allocate-interface vlan101 int1
fwsm/context_name(config)# member gold
fwsm/context_name(config)# config-url tftp://10.1.1.1/contexts/cisco.cfg
fwsm/context_name(config)#  exit
fwsm(config)#
```

Related Commands

Other context submode commands

allocate-interface (context submode)
config-url (context submode)
member (context submode)

Other related commands

class
context
limit-resource (class submode)

context

To create a context and enter the context submode, use the **context** command. To remove the contexts from the running configuration and remove the context entry from the system configuration use the **clear context** command. To delete a single context, use the **no** form of this command.

[**no**] **context** *name*

Syntax Description

name	Name of the context of up to 31 characters.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The FWSM supports 100 contexts.

You cannot enter any context commands until you have created the first context with the **admin-context** command. You cannot remove the current admin context with the **context** command. See the **admin-context** command for more information. The name is limited to 16 characters. This name does not have to match the filename that is specified in the URL.

When you enter the context submode, the following commands are available:

- **allocate-interface**—Indicates the interfaces that are assigned to the context.
- **member**—Indicates class membership for a context.
- **config-url**—Indicates the URL for a context configuration.
- **description**—Provides a description of the context.

Examples

This example shows how to create a context:

```
fwsm(config)# context admincontext
fwsm(config_context)# allocate-interface vlan100 int0
fwsm(config_context)# allocate-interface vlan101 int1
fwsm(config_context)# member gold
fwsm(config_context)# config-url disk:/admin.cfg
fwsm(config_context)# exit
```

Related Commands

admin-context
allocate-interface (context submode)
changeto
class
clear context
config-url (context submode)
description (submode)
member (context submode)
show context

copy capture

To copy a capture file to a TFTP server, use the **copy capture** command.

copy capture: [[**context-name/**] *capture_name* **tftp://server/***pathname* [**pcap**]]

Syntax Description

context-name/	(Optional) Context name.
capture_name	Unique name that identifies the capture.
tftp://server	Specifies the TFTP server.
pathname	Pathname that indicates the last component of the path to the file on the server.
pcap	(Optional) Specifies the defaults of the preconfigured TFTP server.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The FWSM must know how to reach the location (specified by the *tftp_pathname* argument) through its routing table information. This information is determined by the **ip address** command, the **route** command, or the RIP, depending upon the configuration. The *tftp_pathname* can include any directory names in addition to the last component of the path to the file on the server.

The *pathname* can include any directory names in addition to the last component of the path to the file on the server. The pathname cannot contain spaces. If a directory name has spaces, set the directory in the TFTP server instead of in the **copy tftp flash** command.

Note You cannot retrieve images prior to version 2.2 using this feature.

Examples

This example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
fwsm/context_name(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

You can specify the full path as follows:

```
fwsm/context_name(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap pcap
```

If the TFTP server is already configured, the location or filename can be unspecified as follows:

```
fwsm/context_name(config)# tftp-server outside 171.68.11.129 tftp/cdisk
fwsm/context_name(config)# copy capture:abc tftp:/tftp/abc.cap
```

This example shows how to use the defaults of the preconfigured TFTP server in the **copy capture** command:

```
fwsm/context_name(config)# copy capture:abc tftp:pcap
```

Related Commands

cd
clear flashfs
copy disk
copy flash
copy http(s)
copy running-config/copy startup-config
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir
show disk
show file
show flashfs
show http
show running-config
show startup-config
show tftp-server

copy disk

To copy a file from the disk partition to a TFTP server, another location on the disk partition, to the Flash partition, or to the startup or running configuration, use the **copy disk** command.

copy [**/noconfirm**] **disk:**[*path*] **tftp**[**:**[[//server][/*pathname*]]]

copy [**/noconfirm**] **disk:**[*path*] **disk:**[*path*]

copy [**/noconfirm**] **disk:**[*path*] **[flash:**[**image** | **pdm**]

copy [**/noconfirm**] **disk:**[*path*] [**startup-config** | **running-config**]

copy [**/noconfirm**] **disk:**[*path*] **ftp:**//[*user*[*:password*]@] *server* [*pathname*] [**;type=***xx*]

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
path	(Optional) Path to the file location.
tftp	Specifies the TFTP server.
server	(Optional) IP address or name of the server that is set with the **name** command.
pathname	(Optional) Directory path and filename to which to copy.
disk:	Specifies the disk partition that you are copying.
flash	(Optional) Specifies that the copy target is the Flash partition.
image	(Optional) Specifies that the image is copied.
pdm	(Optional) Specifies that a PDM file is copied to the default Flash partition.
startup-config	(Optional) Specifies that a file is copied to the startup configuration.
running-config	(Optional) Specifies that a file is copied to the running configuration.
ftp	Specifies FTP transactions.
user	(Optional) Username for the FTP transfer.
:*password*	(Optional) Password for logging into the FTP server.
@	(Optional) Separates the login information from the server address.
;type=*xx*	(Optional) Specifies the type of transfer. xx is **ap**, **ah**, **ip** (default), or **in.**

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When you copy the image to Flash on the FWSM, the image is not available until you reboot. The downloaded PDM image files are available to the FWSM immediately without a reboot. If you copy a file to the startup partition, you must either reboot or use the **copy start run** command. If you specify TFTP without the **:** (colon), you get a prompt.

Examples

This example shows how to copy a file from the disk to a TFTP server:

```
fwsm/context_name(config)# copy disk:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

This example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
fwsm/context_name(config)# copy disk:my_context.cfg disk:my_context/my_context.cfg
```

This example shows how to copy an image or a PDM file from the disk to the Flash partition:

```
fwsm/context_name(config)# copy disk:cdisk flash:image
fwsm/context_name(config)# copy disk:pdm flash:pdm
```

This example shows how to copy a file from the disk to the startup configuration or a running configuration:

```
fwsm/context_name(config)# copy disk:my_context/my_context.cfg startup-config
fwsm/context_name(config)# copy disk:my_context/my_context.cfg running-config
```

Related Commands

cd
clear flashfs
copy capture
copy flash
copy http(s)
copy running-config/copy startup-config
copy tftp
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir
show disk
show file
show flashfs
show running-config
show startup-config
show tftp-server

copy flash

To copy a file from the Flash partition to a TFTP server, to the disk partition, or to the startup or running configuration, use the **copy flash** command.

copy flash[**:**[**image** | **pdm**]] **tftp**[**:**[[//server][*/pathname*]]]

copy [**/noconfirm**] **flash:**[**image** | **pdm**] **disk:**[*path*]

Syntax Description

image	(Optional) Specifies that the image is copied.
pdm	(Optional) Specifies that a PDM file is copied.
tftp	Specifies the TFTP server.
server	(Optional) IP address or name that you set with the **name** command.
pathname	(Optional) Directory path and filename.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	Specifies that the copy target is the disk partition.
path	(Optional) Path to the file location.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify TFTP without the **:** (colon), you get a prompt.

Examples

This example show how to copy an image or a PDM file from the Flash partition to a TFTP server:

```
fwsm/context_name(config)# copy flash:image tftp://10.7.0.80/image
fwsm/context_name(config)# copy flash:pdm tftp://10.7.0.80/FWSM/pdm
```

This example shows how to copy an image or PDM file from the Flash partition to a disk:

```
fwsm/context_name(config)# copy flash:image disk:cdisk
fwsm/context_name(config)# copy flash:pdm disk:pdm
```

Related Commands

- cd
- clear flashfs
- copy capture
- copy http(s)
- copy running-config/copy startup-config
- copy tftp
- dir
- format
- mkdir
- more
- pwd
- rename
- rmdir
- show disk
- show file
- show flashfs
- show running-config
- show startup-config
- show tftp-server

copy ftp

To copy a file from the Flash partition to a TFTP server, to the disk partition, or to the startup or running configuration, use the **copy flash** command.

copy ftp://[*user*[**:***password*]@] **location/***pathname* [**;type=**<*xx*>] [**startup-config running-config**]

copy [**/noconfirm**] **ftp://**[*user*[**:***password*]@] **location/pathname** [**;type=**<*xx*>] [**startup-config running-config**]

Syntax Description

user	(Optional) Username for logging into the HTTP server.
password@	(Optional) Password for logging into the HTTP server.
location/*pathname*	IP address or name that you set with the **name** command.
;type=*xx*	(Optional) Specifies the type of transfer. xx is **ap**, **ah**, **ip** (default), or **in.**
/noconfirm	(Optional) Specifies not to prompt for confirmation.
startup-config	(Optional) Specifies the startup configuration.
running-config	(Optional) Specifies the running configuration.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify FTP without the **:** (colon), you get a prompt.

Examples

This example shows how to copy a file from the disk to the startup configuration or a running configuration:

```
fwsm/context_name(config)# copy ftp:my_context/my_context.cfg startup-config
fwsm/context_name(config)# copy ftp:my_context/my_context.cfg running-config
```

Related Commands

cd
clear flashfs
copy capture

copy http(s)

To copy files from an HTTPS server, use the **copy http**[**s**] command.

copy http[**s**]**://**[*user***:***password@*] *server* [**:***port*]/*pathname* **flash:**[**image** | **pdm**]

copy [**/noconfirm**] **http**[s]**://**[*user***:***password@*]*location* [**:***port*]/*pathname* **disk:**[*pathname*]

copy http[**s**]**://**[user**:***password@*]*server*[**:***port*]/*pathname* {**startup-config** | **running-config**}

Syntax Description

user	(Optional) Username for logging into the HTTPS server.
password@	(Optional) Password for logging into the HTTPS server.
server	Server name.
location	(Optional) IP address or name that you set with the **name** command.
port	(Optional) Port to contact on the HTTP server.
pathname	(Optional) Name of the resource that contains the FWSM software image or PDM file to copy.
flash	Specifies the location for the download in the Flash partition.
image	(Optional) Downloads the selected FWSM image to the Flash partition.
pdm	(Optional) Downloads the selected PDM image file to the Flash partition.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk	Specifies the location for the download is to disk.
startup-config	(Optional) Specifies the startup configuration.
running-config	(Optional) Specifies the running configuration.

Defaults

The default *port* is 80 for HTTP and 443 for HTTPS.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	This command was introduced
2.2(1)	Support for this command was modified to add the disk, startup and running configuration on the FWSM.

Usage Guidelines

If you specify TFTP without the **:** (colon), you get a prompt.

Examples

This example shows how to copy the FWSM software image from a public HTTP server into the Flash partition of the FWSM:

```
fwsm/context_name(config)# copy http://171.68.11.129/auto/cdisk flash:image
```

This example show how to copy the PDM software image through HTTPS (HTTP over SSL), where the SSL authentication is provided by the username “alice” and the password “xyz”:

```
fwsm/context_name(config)# copy https://alice:xyz@171.68.11.129/auto/pdm.bin flash:pdm
```

This example shows how to copy the FWSM software image from an HTTPS server running on a nonstandard port, where the file is copied into the software image space in the Flash partition by default:

```
fwsm/context_name(config)# copy https://alice:zyx@171.68.11.129:8080/auto/cdisk flash
```

Note When entering the “?” character in a URL, press **Ctrl-v** first.

Related Commands

cd
clear flashfs
copy capture
copy disk
copy flash
copy ftp
copy running-config/copy startup-config
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir
show disk
show file
show flashfs
show running-config
show startup-config
show tftp-server

copy running-config/copy startup-config

To copy the running or startup configuration TFTP or FTP server to the disk partition, use the **copy running-config** or **copy startup-config** command.

copy running-config startup-config

copy startup-config running-config

copy [**startup-config | running-config**] **tftp**[**:**[[**//***location*][**/***pathname*]]]

copy [**/noconfirm**] [**startup-config | running-config**] **disk:**[*path*]

copy [**startup-config | running-config**] **ftp://**[*user*[**:***password*]**@**]*location***/***pathname*[**;type=** *xx*]

Syntax Description

running-config	(Optional) Specifies that a file is copied to the running configuration.
startup-config	(Optional) Specifies that a file is copied to the startup configuration.
tftp	Specifies that the copy is through TFTP.
/location	(Optional) IP address of the server.
/pathname	(Optional) Directory where the files are copied.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	Specifies the copy target is the disk partition.
path	(Optional) Path to the file location.
ftp	Specifies that the copy is through FTP.
user	(Optional) User.
password	(Optional) User password.
;type=*xx*	(Optional) Specifies the type of transfer. xx is **ap**, **ah**, **ip** (default), or **in.**

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify TFTP without the **:** (colon), you get a prompt.

Examples

This example shows how to copy the running configuration to the startup configuration file:

```
fwsm(config)# copy running-config startup-config
```

This example shows how to copy a running configuration file to a TFTP server:

```
fwsm(config)# copy running-config tftp://10.7.0.80/FWSM/my_context/my_context.cfg
```

This example shows how to copy the startup or running configuration to a disk:

```
fwsm(config)# copy startup-config disk:my_context/my_context.cfg
fwsm(config)# copy running-config disk:my_context/my_context.cfg
```

This example shows how to copy the startup configuration to the running configuration:

```
fwsm(config)# copy startup-config running-config
```

This example shows how to copy the startup or running configuration to a TFTP server:

```
fwsm(config)# copy startup-config tftp://10.7.0.80/fwsm#/my_context/my_context.cfg
fwsm(config)# copy running-config tftp://10.7.0.80/fwsm#/my_context/my_context.cfg
```

Related Commands

cd
clear flashfs
copy capture
copy disk
copy flash
copy ftp
copy http(s)
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir
show disk
show file
show flashfs
show running-config
show startup-config
show tftp-server

copy tftp

To download the Flash partition software images through TFTP without using monitor mode, use the **copy tftp** command.

copy tftp:[*//location*][*/pathname*] **flash:**[**image**][**pdm**]

copy[**/noconfirm**] **tftp**[**:**[*//location*][*/pathname*]] **disk:**[*path*]

copy tftp:[**//server**][*/pathname*] {**startup-config** | **running-config**}

Syntax Description

location	(Optional) IP address or name that you set with the **name** command.
pathname	(Optional) Directory path and filename.
flash	Specifies the Flash partition.
image	(Optional) Downloads the selected FWSM image to the Flash partition.
pdm	(Optional) Downloads the selected PDM image files to the Flash partition.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	Specifies that the copy target is the disk partition.
path	(Optional) Path to the file location.
startup-config	(Optional) Specifies that a file is copied to the startup configuration.
running-config	(Optional) Specifies that a file is copied to the running configuration.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	This command was introduced on the FWSM.
2.2(1)	Support was added for disk, startup and tunning configuration options.

Usage Guidelines

The **copy tftp flash** command allows you to download a PDM software image through TFTP. If you specify TFTP without the **:** (colon), you get a prompt.

If the command is used without the **tftp** keyword or *pathname* optional arguments, you are prompted for the server address and filename.

The *pathname* can include any directory names and the last component of the path to the file on the server. The *pathname* cannot contain spaces.

If you configure the TFTP server to point to a directory on the system from which you are downloading the image, you need to use only the IP address of the system and the image filename.

Examples

This example shows how to make the FWSM prompt you for the filename and server before you start the TFTP download:

```
fwsm(config)# copy tftp flash:
Address or name of remote host [127.0.0.1]? 10.1.1.5
Source file name [cdisk]? fwsm.bin
copying tftp://10.1.1.5/fwsm.bin to Flash
[yes|no|again]? yes
!!!!!!!!!!!!!!!!!!!!!!!…
Received 1695744 bytes.
Erasing current image.
Writing 1597496 bytes of image.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!…
Image installed.

fwsm(config)# copy tftp://10.0.0.1/fwsm512.bin flash:
```

This example show how to map an IP address to the TFTP host name with the **name** command and use the **tftp-host** keyword for the *location* argument:

```
fwsm(config)# name 10.1.1.6 tftp-host
fwsm(config)# copy tftp://tftp-host/fwsm512.bin flash:
fwsm(config)# copy tftp://tftp-host/tftpboot/fwsm512.bin flash:
```

This example shows how to copy a file from a TFTP server to a disk. If the file does not fit in the available space, then an error message is printed.

```
fwsm(config)# copy tftp://10.7.0.80/FWSM/my_context.cfg disk:my_context/my_context.cfg
```

Related Commands

cd
clear flashfs
copy capture
copy disk
copy flash
copy ftp
copy http(s)
copy running-config/copy startup-config
dir
format
mkdir
more
pwd
rename
rmdir
show disk
show file
show flashfs
show running-config
show startup-config
show tftp-server

crashdump force

To force a crash of the FWSM, use the **crashdump** command.

crashdump force [**page-fault | watchdog**]

Syntax Description

page-fault	(Optional) Forces a crash of the FWSM with a page fault.
watchdog	(Optional) Forces a crash of the FWSM as a result of watchdogging.

Defaults

The crash information file is saved to the Flash partition.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Caution Be careful entering the **crashdump force** command because it crashes the FWSM and forces it to reload.

The **crashdump force page-fault** command crashes the FWSM as a result of a page fault, and the **crashdump force watchdog** command crashes the FWSM as a result of watchdogging. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashdump force page-fault** or **crashdump force watchdog** command (because these are real crashes). The FWSM reloads after the crash dump is complete.

When you enter the **crashdump force page-fault** command, a warning prompt similar to the following is displayed:

```
fwsm(config)# crashdump force page-fault
WARNING: This command will force the FWSM to crash and reboot.
    Do you wish to proceed? [confirm]:
```

If you enter a carriage return by pressing the Return or enter key, “Y,” or “y,” the FWSM crashes and reloads; all three of these actions are interpreted as confirmation. Any other character is interpreted as a no, and the FWSM returns to the command-line configuration mode prompt.

Related Commands

clear crashdump
failover
show crashdump

crypto dynamic-map

To create a dynamic crypto map entry and enter the crypto dynamic map subcommand mode, use the **crypto dynamic-map** command. Use the **no** form of this command to delete a dynamic crypto map set or entry.

[**no**] **crypto dynamic-map** *map seq*

Syntax Description

map	Name of the dynamic crypto map set.
seq	Sequence number that corresponds to the dynamic crypto map entry.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For more detailed help, refer directly to the CLI subcommand in the mode where they are available; for example: **ca ?** or **help ca**.

Note The **crypto dynamic-map** subcommands are described with the **crypto map client** command. If the peer initiates the negotiation and the local configuration specifies perfect forward secrecy (PFS), the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, a default of group1 is assumed, and an offer of either group1 or group2 is accepted. If the local configuration specifies group2, that group must be part of the peer's offer or the negotiation fails. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

The **crypto dynamic-map** subcommands are as follows:

- **match address** *access_list_name*—See the **crypto map set peer** command.
- **set peer** *ip-address*—See the **crypto map set peer** command.
- **set pfs** [**group1** | **group2**]—See the **crypto map set pfs** command.
- **set security-association lifetime seconds** *seconds* | **kilobytes** *kilobytes*—See the **crypto map set security-association lifetime** command.
- **set transform-set** *proposal* [*proposal ...*]|—See the **crypto map set transform-set** command.

Note The **crypto map set transform-set** command is required for dynamic crypto map entries.

The **crypto dynamic-map** command allows you to create a dynamic crypto map entry. The **no crypto dynamic-map** command deletes a dynamic crypto map set or entry. The **clear crypto dynamic-map** removes all of the **crypto dynamic map** commands. Specifying the name of a given crypto dynamic map removes the associated **crypto dynamic map** commands. You can also specify the dynamic crypto map's sequence number to remove all of the associated **crypto dynamic map** commands. The **show crypto engine** command allows you to see a dynamic crypto map set.

Dynamic crypto maps are policy templates that are used when processing negotiation requests for new security associations from a remote IPSec peer, even if you do not know all of the crypto map parameters that are required to communicate with the peer (such as the peer's IP address). For example, if you do not know about all the remote IPSec peers in the network, a dynamic crypto map lets you accept requests for new security associations from previously unknown peers. (However, these requests are not processed until the Internet Key Exchange (IKE) authentication has completed successfully.)

When the FWSM receives a negotiation request through IKE from another peer, the FWSM examines the request to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, the request is rejected unless the crypto map set includes a reference to a dynamic crypto map.

The dynamic crypto map accepts "wildcard" parameters for any parameters that are not explicitly stated in the dynamic crypto map entry. This situation lets you set up IPSec security associations with a previously unknown peer. (The peer still must specify matching values for the "wildcard" IPSec security association negotiation parameters.)

If the FWSM accepts the peer's request, it installs the new IPSec security associations at the same time that it installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. The FWSM performs normal processing, using this temporary crypto map entry as a normal entry, even when it requests new security associations if the current ones are expiring (based upon the policy specified in the temporary crypto map entry). Once the flow expires (that is, all of the corresponding security associations expire), the temporary crypto map entry is removed.

The **crypto dynamic-map** commands are used for determining whether or not traffic should be protected. The only keyword that is required in a **crypto dynamic-map** command is the **set transform-set** keyword. All other keywords are optional.

Examples

This example shows how to configure an IPSec crypto map set:

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 101
fwsm/context_name(config)# crypto map mymap 10 set transform-set my_t_set1
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
fwsm/context_name(config)# crypto map mymap 20 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 20 match address 102
fwsm/context_name(config)# crypto map mymap 20 set transform-set my_t_set1 my_t_set2
fwsm/context_name(config)# crypto map mymap 20 set peer 10.0.0.3
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10 match address 103
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10 set transform-set my_t_set1
my_t_set2 my_t_set3
fwsm/context_name(config)# crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
```

In the previous example, the crypto map entry **mymap 30** references the dynamic crypto map set **mydynamicmap**, which can be used to process inbound security association negotiation requests that do not match **mymap** entries 10 or 20. In this case, if the peer specifies a transform set that matches one of the transform sets specified in **mydynamicmap** for a flow "permitted" by the access list 103, IPSec accepts the request and sets up security associations with the remote peer without previously knowing about the peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings that are specified by the remote peer.

The access list that is associated with **mydynamicmap 10** is also used as a filter. Inbound packets that match a permit entry in this list are dropped for not being IPSec protected. (The same is true for access lists that are associated with static crypto maps entries.) Outbound packets that match a permit entry without an existing corresponding IPSec security association are also dropped.

Related Commands

clear crypto dynamic-map
show crypto map

crypto ipsec security-association lifetime

To set global lifetime values used when negotiating IPSec security associations, use the **crypto ipsec security-association lifetime** command. To return to the default values, use the **no** form of this command.

[**no**] **crypto ipsec security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

Syntax Description

seconds *seconds*	Specifies the number of seconds that a security association lives before it expires.
kilobytes *kilobytes*	Specifies the volume of traffic (in kilobytes) that passes between IPSec peers using a given security association before that security association expires.

Defaults

The defaults are as follows:

- **seconds** *seconds* is 28,800 seconds (8 hours).
- **kilobytes** *kilobytes* is 4,608,000 KB (10 Mbps for one hour).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For more detailed help, refer directly to the CLI subcommand in the mode where they are available; for example, **ca ?** or **help ca**.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry does not have lifetime values configured, when the FWSM requests new security associations during security association negotiation, it specifies its global lifetime value in the request to the peer. It uses this value as the lifetime of the new security associations. When the FWSM receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a “timed” lifetime and a “traffic-volume” lifetime. The security association expires after either of these lifetimes is reached.

If you change a global lifetime, the change is applied only when the crypto map entry does not have a lifetime value specified. The change is not applied to existing security associations but is used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

To change the global timed lifetime, use the **crypto ipsec security-association lifetime seconds** command. The timed lifetime causes the security association to time out after the specified number of seconds have passed.

To change the global traffic-volume lifetime, use the **crypto ipsec security-association lifetime kilobytes** command. The traffic-volume lifetime causes the security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security associations' key.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key. Shorter lifetimes require more CPU processing time for establishing new security associations. The lifetime values are ignored for manually established security associations (security associations installed using an **ipsec-manual crypto map** command entry).

The security association (and corresponding keys) expires according to whichever occurs sooner, either after the number of seconds has passed (specified by the **seconds** keyword) or after the amount of traffic in kilobytes has passed (specified by the **kilobytes** keyword).

A new security association is negotiated before the lifetime threshold of the existing security association is reached to ensure that a new security association is ready for use when the old one expires. The new security association is negotiated either 30 seconds before the seconds lifetime expires or when the volume of traffic through the tunnel reaches 256 KB less than the **kilobytes** lifetime (whichever occurs first).

If no traffic passes through the tunnel during the entire life of the security association, a new security association is not negotiated when the lifetime expires. Instead, a new security association is negotiated only when IPSec sees another packet that should be protected.

Examples

This example shortens the IPSec SA lifetimes. The time-out lifetime is shortened to 2700 seconds (45 minutes), and the traffic-volume lifetime is shortened to 2,304,000 KB (10 Mbps for 30 minutes).

```
fwsm/context_name(config)# crypto ipsec security-association lifetime seconds 2700
fwsm/context_name(config)# crypto ipsec security-association lifetime kilobytes 2304000
```

Related Commands

clear crypto ipsec sa
show crypto ipsec

crypto ipsec transform-set

To create and configure a transform set, use the **crypto ipsec transform-set** command. To delete a transform set or return to the default transport mode, use the **no** form of this command.

[**no**] **crypto ipsec transform-set** *transform-set-name* {{*transform1* [*transform2* [*transform3*]]} | **mode transport**}

crypto ipsec transform-set *transform-set-name* [**ah-md5-hmac | ah-sha-hmac**] [**esp-des | esp-des-192 | esp-des-256 | esp-des | esp-3des | esp-null**] [**esp-md5-hmac | esp-sha-hmac**]

Syntax Description

transform-set-name	Name of the transform set to create or modify.
transform1 *transform2* *transform3*	Up to three transforms to create or modify.
mode transport	Specifies that the FWSM negotiate with a Windows 2000 Layer 2 TP/IPSec client.
ah-md5-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using MD5.
ah-sha-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using SHA.
esp-des	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a 128-bit key.
esp-des-192	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a 192-bit key.
esp-des-256	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a 256-bit key.
esp-null	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a null key.
esp-md5-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with a md5 key.
esp-sha-hmac	(Optional) Specifies that the IPSec messages that are protected by this transform are encrypted using des and 3des with an sha key.

Defaults

Tunnel mode

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Transforms define the IPSec security protocol(s) and algorithm(s). Each transform represents an IPSec security protocol (Encapsulating Security Payload (ESP), authenticating header (AH), or both) and the algorithm that you want to use.

The Windows 2000 Layer 2 Tunneling Protocol (L2TP)/IPSec client uses IPSec transport mode, so **transport** mode must be selected on the transform set. For FWSM version 1.1 and later releases, L2TP is the only protocol that can use the IPSec transport mode. All other types of packets using IPSec transport mode are discarded by the FWSM.

Note A transport mode transform can only be used on a **dynamic** crypto map, and the FWSM CLI displays an error if you attempt to tie a transport-mode transform to a **static** crypto map.

Tunnel mode is automatically enabled for a transform set, so you do not have to explicitly configure the **mode** when tunnel mode is desired.

A transform set specifies one or two IPSec security protocols (either ESP or AH or both) and specifies which algorithms to use with the selected security protocol. During the IPSec security association negotiation, the peers agree to use a particular transform set when protecting a particular data flow.

IPSec messages can be protected by a transform set using des and 3des with a 128-bit key, 192-bit key, or 256-bit key.

This example uses the des and 3des 192-bit key transform:

```
fwsm(config)# crypto ipsec transform-set standard esp-des-192 esp-md5-hmac
```

Note Des and 3des support is available on the FWSMs that are licensed for VPN-3DES only.

You can configure multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The transform set that is defined in the crypto map entry is used in the IPSec security association negotiation to protect the data flows specified by that crypto map entry's access list. During the negotiation, the peers search for a transform set that is the same at both peers. When a transform set is found, it is selected and is applied to the protected traffic as part of both peer's IPSec security associations.

When security associations are established manually, you must use a single transform set. The transform set is not negotiated.

Before a transform set can be included in a crypto map entry, you must defined it by entering the **crypto ipsec transform-set** command.

To define a transform set, you specify one to three "transforms"—each transform represents an IPSec security protocol (ESP or AH) and the algorithm that you want to use. When the particular transform set is used during negotiations for IPSec security associations, the entire transform set (the combination of protocols, algorithms, and other settings) must match a transform set at the remote peer.

In a transform set, you can specify the AH protocol or the ESP protocol. If you specify an ESP protocol in a transform set, you can specify just an ESP encryption transform or both an ESP encryption transform and an ESP authentication transform.

Examples of acceptable transform combinations are as follows:

- **ah-md5-hmac**
- **esp-des**
- **esp-des** and **esp-md5-hmac**
- **ah-sha-hmac** and **esp-des** and **esp-sha-hmac**

If you specify one or more transforms in the **crypto ipsec transform-set** command for an existing transform set, the specified transforms replace the existing transforms for that transform set.

If you change a transform set definition, the change is applied only to crypto map entries that reference the transform set. The change is not applied to existing security associations but is used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

Examples

This example defines one transform set (named "standard"), which is used with an IPSec peer that supports the ESP protocol. Both an ESP encryption transform and an ESP authentication transform are specified in this example.

```
fwsm(config)# crypto ipsec transform-set standard esp-des esp-md5-hmac
```

Related Commands

show crypto ipsec

crypto map client

To create or modify a crypto map entry, use the **crypto map client** command. To return to the default settings, use the **no** form of this command.

crypto map *map-name* **client** [**token**] **authentication** *aaa-server-name*

crypto map *map-name* **client authentication** *aaa-server-name* [**LOCAL**]

crypto map *map-name* **client configuration address** {**initiate** | **respond**}

no crypto map *map-name* **client**

Syntax Description

map-name	Name of the crypto map set.
token	(Optional) Indicates a token-based server for user authentication.
authentication	(Optional) Indicates that the key string is to be used with the ESP authentication transform.
aaa-server-name	Name of the AAA server that will authenticate the user during Internet Key Exchange (IKE) authentication; valid values are **TACACS+**, **RADIUS**, or **LOCAL**.
LOCAL	(Optional) Specifies a predefined server tag for the AAA local protocol.
configuration address	Configures the IKE mode configuration.
initiate	Indicates that the FWSM will attempt to set IP addresses for each peer.
respond	Indicates that the FWSM will accept requests for IP addresses from any requesting peer.

Defaults

The default settings are as follows:

- Xauth feature is not enabled.
- IKE mode configuration is not enabled.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **crypto map client authentication** command allows you to enable the Extended Authentication (Xauth) feature. This feature lets you prompt for a TACACS+, RADIUS, or LOCAL username and password during IKE authentication. You must first set up the AAA server configuration to use this feature, and be sure to specify the same AAA server name within the **crypto map client authentication** command as was specified in the **aaa-server** command. This command is required only when the crypto map entry's transform set includes an Encapsulation Security Payload (ESP) authentication transform.

You can enter the **LOCAL** optional keyword for the group tag value and use the local FWSM database AAA services such as local command authorization privilege levels. LOCAL is the only second authentication method. The **authorization** command only accepts the LOCAL option when the *server_tag* refers to an existing and valid AAA TACACS+ or RADIUS server group defined in an **aaa-server** configuration command.

This command tells the FWSM during Phase 1 of IKE to use the Xauth (RADIUS, TACACS+, or LOCAL) challenge to authenticate IKE. If the Xauth fails, the IPSec security association is not established, and the IKE security association is deleted. Use the **no crypto map client authentication** command to restore the default value. The Xauth feature is not enabled by default.

Note When Xauth is enabled, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. However, when using Xauth with the Easy VPN Remote feature in network extension mode, the IPSec tunnel is created from network to network, so that the users behind the FWSM cannot be associated with a single IP address. A uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the FWSM. For more information on AAA authentication proxies, see the **aaa** commands.

You cannot enable Xauth or IKE mode configuration on an interface when terminating a Layer 2 Tunneling Protocol (L2TP)/IPSec tunnel using the Microsoft L2TP/IPSec client v1.0 (which is available on Windows NT, Windows XP, Windows 98, and Windows ME OS). Instead, you can do either of the following:

- Use a Windows 2000 L2TP/IPSec client.
- Use the **isakmp key** *keystring* **address** *ip-address* **netmask** *mask* **no-xauth no-config-mode** command to exempt the L2TP client from Xauth and IKE mode configuration. However, if you exempt the L2TP client from Xauth or IKE mode configuration, all the L2TP clients must be grouped with the same ISAKMP preshared key or certificate and have the same fully qualified domain name.

The **crypto map client token authentication** command allows you to enable the FWSM to interoperate with a Cisco VPN 3000 Client that is set up to use a token-based server for user authentication. The **token** keyword tells the FWSM that the AAA server uses a token-card system and to prompt the user for the username and password during IKE authentication. Enter the **no crypto map client token authentication** command to restore the default value.

Note The remote user must run Cisco VPN Client version 3.x, Cisco VPN 3000 Client version 2.5/2.6 or higher, or Cisco Secure VPN Client version 1.1 or higher.

The AAA server optional keywords that are available are TACACS+, RADIUS, or LOCAL.

If you specify **LOCAL** and the local user credential database is empty, this message displays:

```
Warning:local database is empty! Use \Qusername' command to define local users.
```

If the local database becomes empty when LOCAL is still present in the command, this message displays:

```
Warning:Local user database is empty and there are still commands using LOCAL for
authentication.
```

The **crypto map client configuration address** command allows you to configure IKE mode configuration on the FWSM. IKE mode configuration allows the FWSM to download an IP address to the remote peer (client) as part of an IKE negotiation. When you enter the **crypto map client configuration address** command, you define the crypto map(s) that should attempt to configure the peer.

The **initiate** keyword indicates that the FWSM will attempt to set IP addresses for each peer. The **respond** keyword indicates that the FWSM will accept requests for IP addresses from any requesting peer.

Note If you use IKE mode configuration on the FWSM, the routers handling the IPSec traffic must also support IKE mode configuration. Cisco IOS Release 12.0(6)T and later releases support IKE mode configuration.

Examples

This example shows how to set up the IPSec rules for VPN encryption IPSec. The **ip**, **nat**, and **aaa-server** commands establish the context for the IPSec-related commands.

```
fwsm/context_name(config)# ip address inside 10.0.0.1 255.255.255.0
fwsm/context_name(config)# ip address outside 168.20.1.5 255.255.255.0
fwsm/context_name(config)# dealer 10.1.2.1-10.1.2.254
fwsm/context_name(config)# nat (inside) 0 access-list 80
fwsm/context_name(config)# aaa-server TACACS+ protocol tacacs+
fwsm/context_name(config)# aaa-server TACACS+ (inside) host 10.0.0.2 secret123
fwsm/context_name(config)# crypto ipsec transform-set pc esp-des esp-md5-hmac
fwsm/context_name(config)# crypto dynamic-map cisco 4 set transform-set pc
fwsm/context_name(config)# crypto map partner-map 20 ipsec-isakmp dynamic cisco
fwsm/context_name(config)# crypto map partner-map client configuration address initiate
fwsm/context_name(config)# crypto map partner-map client authentication TACACS+
fwsm/context_name(config)# crypto map partner-map interface outside
fwsm/context_name(config)# isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0
fwsm/context_name(config)# isakmp client configuration address-pool local dealer outside
fwsm/context_name(config)# isakmp policy 8 authentication pre-share
fwsm/context_name(config)# isakmp policy 8 encryption des
fwsm/context_name(config)# isakmp policy 8 hash md5
fwsm/context_name(config)# isakmp policy 8 group 1
fwsm/context_name(config)# isakmp policy 8 lifetime 86400
```

This example shows how to configure IKE mode configuration on the FWSM:

```
fwsm/context_name(config)# crypto map mymap client configuration address initiate
fwsm/context_name(config)# crypto map mymap client configuration address respond
```

Related Commands

crypto map interface
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map interface

To apply a previously defined crypto map set to an interface, use the **crypto map interface** command. To remove the crypto map set from the interface, use the **no** form of this command.

[**no**] **crypto map** *map-name* **interface** *interface-name*

Syntax Description

map-name	Name of the crypto map set.
interface *interface-name*	Specifies the identifying interface to be used by the FWSM to identify itself to peers.

Defaults

The default settings are as follows:

- Xauth feature is not enabled.
- Internet Key Exchange (IKE) mode configuration is not enabled.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **crypto map interface** command allows you to assign a crypto map set to any active FWSM interface. The FWSM supports IPSec termination on any and all active interfaces. You must assign a crypto map set to an interface before that interface can provide IPSec services.

Only one crypto map set can be assigned to an interface. If multiple crypto map entries have the same *map-name* but a different *seq-num*, they are considered to be part of the same set and will all be applied to the interface. The crypto map entry with the lowest *seq-num* is considered the highest priority and is evaluated first. A single crypto map set can contain a combination of ipsec-isakmp and ipsec-manual crypto map entries.

Caution Using the **crypto map interface** command reinitializes the security association database and causes any currently established security associations to be deleted.

If you enable IKE, and you are using a certification authority (CA) to obtain certificates, you must enable IKE with the interface address that is specified in the CA certificates.

Examples

This example assigns the crypto map set “mymap” to the outside interface. When traffic passes through the outside interface, the traffic is evaluated against all the crypto map entries in the “mymap” set. When outbound traffic matches an access list in one of the “mymap” crypto map entries, a security association (if IPSec) is established if no security association or connection already exists.

```
fwsm/context_name(config)# crypto map mymap interface outside
```

Related Commands

crypto map client
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map ipsec

To create or modify a crypto map entry, use the **crypto map ipsec** command. To delete a crypto map entry or set, use the **no** form of this command.

[**no**] **crypto map** *map-name seq-num* {**ipsec-isakmp** | **ipsec-manual**}
[**dynamic** *dynamic-map-name*]

Syntax Description

map-name	Name of the crypto map set.
seq-num	Number used to rank multiple crypto map entries within a crypto map set.
ipsec-isakmp	Specifies an ipsec-isakmp crypto map entry.
ipsec-manual	Specifies an ipsec-manual crypto map entry.
dynamic *dynamic-map-name*	(Optional) Specifies that a given crypto map entry is to reference a specified dynamic crypto map.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

After you define crypto map entries, you can use the **crypto map interface** command to assign the crypto map set to interfaces.

Crypto maps can filter or classify traffic to be protected and define the policy to be applied to that traffic. The first use affects the flow of traffic on an interface; the second affects the negotiation performed through the IKE on behalf of that traffic.

IPSec crypto maps link together definitions of the following:

- What traffic should be protected
- IPSec peer(s) to which the protected traffic can be forwarded—these are the peers with which a security association can be established
- Which transform sets are acceptable for use with the protected traffic
- How keys and security associations should be used/managed (or what the keys are if IKE is not used)

A crypto map set is a collection of crypto map entries each with a different *seq-num* but the same *map-name*. For a given interface, you could have certain traffic forwarded to one peer with specified security applied to that traffic, and other traffic forwarded to the same or a different peer with different IPSec security applied. To accomplish this situation, you would create two crypto map entries, each with the same *map-name*, but each with a different *seq-num*.

The number that you assign to the *seq-num* argument should not be arbitrary. This number is used to rank multiple crypto map entries within a crypto map set. Within a crypto map set, a crypto map entry with a lower seq-num is evaluated before a map entry with a higher seq-num; that is, the map entry with the lower number has a higher priority.

Use the **crypto dynamic-map** command to create dynamic crypto map entries. After you create a dynamic crypto map set, use the **crypto map ipsec-isakmp dynamic** command to add the dynamic crypto map set to a static crypto map.

Give the lowest priority map entries to the crypto map entries that reference the dynamic map set. This action allows the inbound security association negotiation requests to try to match the static maps first. If the request does not match any of the static maps, set the entries to be evaluated against the dynamic map set.

To make a crypto map entry that references a dynamic crypto map to be set to the lowest priority map entry, give the map entry the highest *seq-num* of all the map entries in a crypto map set.

Examples

This example shows the minimum required crypto map configuration when IKE is used to establish the security associations:

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 101
fwsm/context_name(config)# crypto map mymap set transform-set my_t_set1
fwsm/context_name(config)# crypto map mymap set peer 10.0.0.1
```

This example shows the minimum required crypto map configuration when the security associations are manually established:

```
fwsm/context_name(config)# crypto transform-set someset ah-md5-hmac esp-des
fwsm/context_name(config)# crypto map mymap 10 ipsec-manual
fwsm/context_name(config)# crypto map mymap 10 match address 102
fwsm/context_name(config)# crypto map mymap 10 set transform-set someset
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.5
fwsm/context_name(config)# crypto map mymap 10 set session-key inbound ah 256
9876543210987654987654321098765 4
fwsm/context_name(config)# crypto map mymap 10 set session-key outbound ah 256
fedcbafedcbafedcfedcbafedcbafedc
fwsm/context_name(config)# crypto map mymap 10 set session-key inbound esp 256 cipher
0123456789012345
fwsm/context_name(config)# crypto map mymap 10 set session-key outbound esp 256 cipher
abcdefabcdefabcd
```

This example configures an IPSec crypto map set that includes a reference to a dynamic crypto map set.

Crypto map “mymap 10” allows security associations to be established between the FWSM and either (or both) of two remote IPSec peers for traffic matching access list 101. Crypto map “mymap 20” allows either of two transform sets to be negotiated with the peer for traffic matching access list 102.

Crypto map entry “mymap 30” references the dynamic crypto map set “mydynamicmap,” that can be used to process inbound security association negotiation requests that do not match “mymap” entries 10 or 20. If the peer specifies a transform set that matches one of the transform sets that are specified in “mydynamicmap” for a flow “permitted” by the access list 103, IPSec accepts the request and sets up

security associations with the peer without previously knowing about the peer. If accepted, the resulting security associations (and temporary crypto map entry) are established according to the settings specified by the peer.

The access list that is associated with "mydynamicmap 10" is also used as a filter. Inbound packets that match a permit statement in this list are dropped for not being IPSec protected. (The same is true for access lists that are associated with static crypto maps entries.) Outbound packets that match a permit entry without an existing corresponding IPSec security association are also dropped.

This example shows the configuration using "mydynamicmap":

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 101
fwsm/context_name(config)# crypto map mymap 10 set transform-set my_t_set1
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.1
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.2
fwsm/context_name(config)# crypto map mymap 20 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 102
fwsm/context_name(config)# crypto map mymap 10 set transform-set my_t_set1 my_t_set2
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.3
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10 match address 103
fwsm/context_name(config)# crypto dynamic-map mydynamicmap 10 set transform-set my_t_set1
my_t_set2 my_t_set3
fwsm/context_name(config)# crypto map mymap 30 ipsec-isakmp dynamic mydynamicmap
```

Related Commands

crypto map client
crypto map interface
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set peer

To specify an IPSec peer in a crypto map entry, use the **crypto map set peer** command. To remove an IPSec peer from a crypto map entry, use the **no** form of this command.

[**no**] **crypto map** *map-name seq-num* **set peer** {*hostname* | *ip-address*}

Syntax Description

map-name	Name of the crypto map set.
seq-num	Number used to rank multiple crypto map entries within a crypto map set.
hostname	Name of the host.
ip-address	IP address of the host.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is required for all the static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required and in most cases is not used because the peer is unknown.

For ipsec-isakmp crypto map entries, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that sent either traffic or a negotiation request for a given data flow to the FWSM. If the attempt fails with the first peer, Internet Key Exchange (IKE) tries the next peer on the crypto map list.

For ipsec-manual crypto entries, you can specify only one peer per crypto map. If you want to change the peer, you must delete the old peer and then specify the new peer.

Examples

This example shows a crypto map configuration when IKE is used to establish the security associations. In this example, a security association could be set up to either the peer at 10.0.0.1 or the peer at 10.0.0.2.

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 101
fwsm/context_name(config)# crypto map mymap 10 set transform-set my_t_set1
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set pfs
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set pfs

To set the IPSec to ask for perfect forward secrecy (PFS) when requesting new security associations or to require PFS when receiving requests for new security associations, use the **crypto map set pfs** command. To specify that IPSec should not request PFS, use the **no** form of this command.

[**no**] **crypto map** *map-name seq-num* **set pfs** [**group1 | group2**]

Syntax Description

map-name	Name of the crypto map set.
seq-num	Number used to rank multiple crypto map entries within a crypto map set.
set pfs	Specifies PFS.
group1	(Optional) Specifies a Diffie-Hellman prime modulus group.
group2	(Optional) Specifies a Diffie-Hellman prime modulus group.

Defaults

The defaults are as follows:

- PFS is not requested.
- **group1**.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is available only for ipsec-isakmp crypto map entries and dynamic crypto map entries.

With PFS, every time that a new security association is negotiated, a new Diffie-Hellman exchange occurs, which requires additional processing time. PFS adds another level of security. If one key is ever deciphered by an attacker, only the data that is sent with that key is compromised.

During negotiation, this command causes IPSec to request PFS when requesting new security associations for the crypto map entry. The default (group1) is sent if the **set pfs** command does not specify a group.

If the peer initiates the negotiation and the local configuration specifies PFS, the peer must perform a PFS exchange or the negotiation fails. If the local configuration does not specify a group, a default of group1 is assumed, and an offer of either group1 or group2 is accepted. If the local configuration specifies group2, that group must be part of the peer's offer or the negotiation fails. If the local configuration does not specify PFS, it accepts any offer of PFS from the peer.

The 1024-bit Diffie-Hellman prime modulus group, group2, provides more security than group1 but requires more processing time than group1.

Note Internet Key Exchange (IKE) negotiations with a remote peer may hang when a FWSM has numerous tunnels that originate from the FWSM and terminate on a single remote peer. This problem occurs when PFS is not enabled, and the local peer requests many simultaneous rekey requests. If this problem occurs, the IKE security association will not recover until it has timed out or until you manually clear it with the **clear** [**crypto**] **isakmp sa** command. The FWSM units that are configured with many tunnels to many peers or many clients sharing the same tunnel are not affected by this problem. If the configuration is affected, enable PFS with the **crypto map** *mapname seqnum* **set pfs** command.

Examples

This example specifies that PFS should be used whenever a new security association is negotiated for the crypto map "mymap 10":

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 set pfs group2
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set security-association lifetime

To override (for a particular crypto map entry) the global lifetime value that is used when negotiating IPSec security associations, use the **crypto map set security-association lifetime** command. To reset a crypto map entry's lifetime value to the global value, use the **no** form of this command.

[**no**] **crypto map** *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

Syntax Description

map-name	Name of the crypto map set.
seq-num	Number used to rank multiple crypto map entries within a crypto map set.
seconds *seconds*	Sets the keys and security association to time out after the specified number of seconds have passed.
kilobytes *kilobytes*	Sets the keys and security association to time out after the specified amount of traffic (in kilobytes) has been protected by the security association's key.

Defaults

The defaults are as follows:

- **seconds** *seconds* is 28,800 seconds (8 hours).
- **kilobytes** *kilobytes* is 4,608,000 KB (10 MBPS for one hour).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The crypto map's security associations are negotiated according to the global lifetimes.

This command is available only for ipsec-isakmp crypto map entries and dynamic crypto map entries.

IPSec security associations use shared secret keys. These keys and their security associations time out together.

Assuming that the particular crypto map entry has lifetime values configured, when the FWSM requests new security associations during security association negotiation, it specifies its crypto map lifetime value in the request to the peer; it uses this value as the lifetime of the new security associations. When the FWSM receives a negotiation request from the peer, it uses the smaller of the lifetime values proposed by the peer or the locally configured lifetime value as the lifetime of the new security associations.

There are two lifetimes: a "timed" lifetime and a "traffic-volume" lifetime. The session keys/security association expires after either of these lifetimes is reached.

If you change a lifetime, the change is not applied to existing security associations but is used in subsequent negotiations to establish security associations for data flows that are supported by this crypto map entry. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

Shorter lifetimes can make it harder to mount a successful key recovery attack, because the attacker has less data encrypted under the same key. Shorter lifetimes require more CPU processing time.

The lifetime values are ignored for manually established security associations (security associations installed through an ipsec-manual crypto map entry).

Examples

This example shortens the timed lifetime for a particular crypto map entry because there is a higher risk that the keys could be compromised for security associations belonging to the crypto map entry. The traffic-volume lifetime is not changed because there is not a high volume of traffic anticipated for these security associations. The timed lifetime is shortened to 2700 seconds (45 minutes).

```
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto security-association lifetime seconds 2700
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set session-key
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set session-key

To manually specify the IPSec session keys within a crypto map entry, use the **crypto map set session-key** command. To remove IPSec session keys from a crypto map entry, use the **no** form of this command.

[**no**] **crypto map** *map-name seq-num* **set session-key** {**inbound** | **outbound**} **ah** *spi hex-key-string*

crypto map *map-name seq-num* **set session-key** {**inbound** | **outbound**} **esp** *spi* **cipher** *hex-key-string* [**authenticator** *hex-key-string*]

Syntax Description

map-name	Name of the crypto map set.
seq-num	Number used to rank multiple crypto map entries within a crypto map set.
inbound	Specifies inbound traffic.
outbound	Specifies outbound traffic.
ah	Specifies the Authorization Header (AH) protocol.
spi	Security Parameter Index (SPI) number.
hex-key-string	Hexadecimal key string that is associated with the SPI number.
esp	Specifies the Encapsulation Security Payload (ESP) encryption protocol.
cipher	Specifies cipher encoding.
authenticator	(Optional) Specifies ESP authentication.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is available only for ipsec-manual crypto map entries.

If the crypto map's transform set includes an AH protocol, you must define IPSec keys for AH for both inbound and outbound traffic. If the crypto map's transform set includes an ESP encryption protocol, you must define IPSec keys for ESP encryption for both inbound and outbound traffic. If the crypto map's transform set includes an ESP authentication protocol, you must define IPSec keys for ESP authentication for inbound and outbound traffic.

When you define multiple IPSec session keys within a single crypto map, you can assign the same Security Parameter Index (SPI) number to all the keys. The SPI is used to identify the security association that is used with the crypto map. However, not all the peers have the same flexibility in SPI assignment.

You may have to coordinate the SPI assignment with the peer's network administrator, making sure that the same SPI is not used more than once for the same destination address/protocol combination.

Security associations that are established using this command do not expire—unlike security associations established using the IKE.

The FWSM's session keys must match its peer's session keys.

If you change a session key, the security association using the key is deleted and reinitialized.

Examples

This example shows a crypto map entry for manually established security associations. The transform set "t_set" includes only an AH protocol.

```
fwsm/context_name(config)# crypto ipsec transform-set t_set ah-sha-hmac
fwsm/context_name(config)# crypto map mymap 20 ipsec-manual
fwsm/context_name(config)# crypto map mymap 20 match address 102
fwsm/context_name(config)# crypto map mymap 20 set transform-set t_set
fwsm/context_name(config)# crypto map mymap 20 set peer 10.0.0.21
fwsm/context_name(config)# crypto map mymap 20 set session-key inbound ah 300
1111111111111111111111111111111111111111
fwsm/context_name(config)# crypto map mymap 20 set session-key outbound ah 300
2222222222222222222222222222222222222222
```

This example shows a crypto map entry for manually established security associations. The transform set "someset" includes both an AH and an ESP protocol, so session keys are configured for both AH and ESP for both inbound and outbound traffic. The transform set includes both encryption and authentication ESP transforms. Session keys are created for both using the **cipher** and **authenticator** keywords.

```
fwsm/context_name(config)# crypto ipsec transform-set someset ah-sha-hmac esp-des
esp-sha-hmac
fwsm/context_name(config)# crypto map mymap 10 ipsec-manual
fwsm/context_name(config)# crypto map mymap 10 match address 101
fwsm/context_name(config)# crypto map mymap 10 set transform-set someset
fwsm/context_name(config)# crypto map mymap 10 set peer 10.0.0.1
fwsm/context_name(config)# crypto map mymap 10 set session-key inbound ah 300
9876543210987654321098765432109876543210
fwsm/context_name(config)# crypto map mymap 10 set session-key outbound ah 300
fedcbafedcbafedcbafedcbafedcbafedc
fwsm/context_name(config)# crypto map mymap 10 set session-key inbound esp 300 cipher
0123456789012345
    authenticator 00001111222233334444555566667777888899999
fwsm/context_name(config)#  crypto map mymap 10 set session-key outbound esp 300 cipher
abcdefabcdefabcd
    authenticator 99998888777766665555444433332222111110000
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set transform-set
crypto map set peer
show crypto map

crypto map set transform-set

To specify a list of transform sets in priority order, use the **crypto map set transform-set** command. To remove all the transform sets from a crypto map entry, use the **no** form of this command.

[**no**] **crypto map set transform-set** *proposal* [*proposal* ...]

Syntax Description

proposal	Proposal tag.
proposal...	(Optional) Proposal tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is required for all the static and dynamic crypto map entries.

For an **ipsec-isakmp crypto map** entry, you can list up to six transform sets with this command. List the higher priority transform sets first.

If the local FWSM initiates the negotiation, the transform sets are presented to the peer in the order that is specified in the **crypto map** command. If the peer initiates the negotiation, the local FWSM accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec does not establish a security association and the traffic is dropped.

For an **ipsec-manual crypto map** command, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

To change the list of transform sets, respecify the new list of transform sets to replace the old list. This change is applied only to **crypto map** commands that reference this transform set. The change is not applied to existing security associations but is used in subsequent negotiations to establish new security associations. To make the new settings take effect sooner, you can clear all or part of the security association database by using the **clear crypto ipsec sa** command.

Any transform sets that are included in the **crypto map** command must previously have been defined using the **crypto ipsec transform-set** command.

Examples

This example shows how to display the transform sets:

```
fwsm/context_name(config)# crypto map transform-set
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set session-key
crypto map set peer
show crypto map

crypto match address

To specify the match address of packets to encrypt, use the **crypto match address** command. To remove the access list from a crypto map entry, use the **no** form of this command.

[**no**] **crypto match address** *access_list_name*

Syntax Description

access_list_name	Name of the access list.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is required for all the static crypto map entries. If you are defining a dynamic crypto map entry (with the **crypto dynamic-map** command), this command is not required but is strongly recommended.

Use the **access-list extended** command to define this access list.

The access list that is specified with this command is used by IPSec to determine which traffic should be protected by IPSec crypto and which traffic does not need protection. Traffic that is permitted by the access list is protected. Traffic that is denied by the access list is not protected.

Note The crypto access list is not used to determine whether to permit or deny traffic through the interface. An access list that is applied directly to the interface with the **access-group** command makes that determination.

The crypto access list that is specified by this command is used when evaluating both inbound and outbound traffic. Outbound traffic is evaluated against the crypto access lists that are specified by the interface's crypto map entries to determine if it should be protected by crypto, and if so, which crypto policy applies. For IPSec crypto maps, new security associations are established using the data flow identity that is specified in the permit entry. For dynamic crypto map entries, if no security association exists, the packet is dropped. Inbound traffic is evaluated against the crypto access lists that are specified by the entries of the interface's crypto map set to determine if it should be protected by crypto and, if so, which crypto policy applies. (For IPSec, unprotected traffic is discarded because it should have been protected by IPSec.)

The access list is used to identify the flow for which the IPSec security associations are established. For outbound traffic, the permit entry is used as the data flow identity. For inbound traffic, the data flow identity that is specified by the peer must be "permitted" by the crypto access list.

Examples

This example shows how to specify the match address of packets to encrypt:

```
fwsm/context_name(config)# crypto match address 101
```

Related Commands

crypto map client
crypto map interface
crypto map ipsec
crypto map set peer
crypto map set pfs
crypto map set security-association lifetime
crypto map set session-key
crypto map set transform-set
show crypto map

debug

To debug packets or ICMP tracings to the interface to provide information for troubleshooting, use the **debug** command. To disable debugging, use the **no** form of this command.

[**no**] **debug** *command*

[**no**] **debug packet** *interface_name* [**src** *s_ip* [**netmask** *m*]] [**dst** *d_ip* [**netmask** *m*]] [[**proto icmp**] | [**proto tcp** [**sport** *s_p*] [**dport** *d_p*]] [**proto udp** [**sport** *s_p*] [**dport** *d_p*]] [**rx** | **tx** | **both**]

Syntax Description

Table 2-5, Table 2-6, and Table 2-7 list the syntax descriptions for the **debug** command.

Table 2-5 Debug Arguments and Keywords

Syntax	Description
interface_name	Interface name.
s_ip	(Optional) Source IP address.
m	(Optional) Network mask.
d_ip	(Optional) Destination IP address.
proto icmp	(Optional) Displays ICMP packets only.
proto tcp	(Optional) Displays TCP packets only.
s_p	(Optional) Source port.
d_p	(Optional) Destination port.
proto udp	(Optional) Displays UDP packets only.
sport	(Optional) Source port.
dport	(Optional) Destination port.
rx	(Optional) Displays only packets received at the FWSM firewall.
tx	(Optional) Displays only packets transmitted from the FWSM firewall.
both	(Optional) Displays both received and transmitted packets.

Table 2-6 debug Commands Without Arguments or Keywords

Syntax	Description
debug arp-inspection	Displays information about ARP inspection.
debug arp-np	Displays information about ARP NP.
debug context	Displays informaiton about contexts.
debug ftp client	Displays informaiton about the FTP client.
debug icmp trace	Displays information about ICMP traffic.
debug ils	Displays Internet Locator Service (ILS) fixup information (used in LDAP services).
debug l2-indication	Displays informaiton about Layer 2.
debug mac-address-table	Displays informaiton about the MAC address table.

Table 2-6 debug Commands Without Arguments or Keywords (continued)

Syntax	Description
debug pdm history	Displays history informaiton about the PDM.
debug rip	Displays informaiton about RIP.
debug route-np	Displays information from the FWSM routing module.
debug rtsp	Displays information about RTSP.
debug sequence	Displays informaiton about sequence.
debug sip	Debugs the fixup Session Initiation Protocol (SIP) module.
debug skinny	Debugs SCCP protocol activity. (Using this command may impact performance on high-traffic network segments.)
debug sqlnet	Debugs SQL*Net traffic.
debug ssh	Debugs information and error messages that are associated with the **ssh** command.
debug sunrpc	Displays informaiton about the Sun RPC.
debug timestamps	Displays informaiton about timestamps.
debug xlate	Displays informaiton about xlates.
no debug all	Stops any and all debug messages from being displayed.
undebug all	Stops any and all debug messages from being displayed.

Table 2-7 debug Commands With Arguments or Keywords

Syntax	Syntax Description
debug aaa [**authentication** | **authorization** | **accounting** | **internal**]	Displays authentication, authorization, and accounting information. **authentication**—(Optional) Specifies AAA authentication information. **authorization**—(Optional) Specifies AAA authorization information. **accounting**—(Optional) Specifies AAA accounting information. **internal**—(Optional) Specifies AAA internal information.
debug acl [**config** | **download** | **trace -error** | **tree-sync**]	Displays access list configuration information.
debug aging [**stop** | **restart**]	

Table 2-7 debug Commands With Arguments or Keywords (continued)

Syntax	Syntax Description
debug crypto [**ipsec** | **isakmp** | **ca** | **engine**] [*level*]	Displays crypto information. **ca**—Displays information about certification authority (CA) traffic. **ipsec**—Displays information about IPSec traffic. **isakmp**—Displays information about Internet Key Exchange (IKE) traffic. **vpnclient**—Displays information about the FWSM EasyVPN client. *level*—(Optional) Specifies the level of the debugging feedback. The higher the level number, the more information is displayed. The default *level* is 1. The levels correspond to the following events: • Level 1: Interesting events • Level 2: Normative and interesting events • Level 3: Diminutive, normative, and interesting events
debug dhcpd {**event** | **packet**}	Displays Dynamic Host Configuration Protocol (DHCP) server information. **event**—Displays event information that is associated with the DHCP server. **packet**—Displays packet information that is associated with the DHCP server.
debug dhcprelay {**event** | **packet** | **error**}	Displays DHCP relay agent information. **event**—Displays event information that is associated with the DHCP relay agent. **packet**—Displays packet information that is associated with the DHCP relay agent. **error**—Displays error messages that are associated with the DHCP relay agent.
debug disk [**file** | **filesystem** | **file-verbose**]	
debug dns {**resolver** | **all**}	Displays Domain Name Server (DNS) debugging information. **resolver**—Displays DNS resolution information. **all**—Displays all DNS information.
debug fixup {**udp** | **tcp**}	Displays fixup information. **udp**—Displays fixup information using UDP. **tcp**—Displays fixup information using TCP.
debug fover *option*	Displays failover information. *option*—Displays failover information. See Table 2-8 for the optional keywords.

Table 2-7 debug Commands With Arguments or Keywords (continued)

Syntax	Syntax Description
debug h323 {**h225** | **h245** | **ras**} [**asn** | **event**]	Displays information about the packet-based multimedia communications systems standard. **h225**—Specifies H.225 signaling. **h245**—Specifies H.245 signaling. **ras**—Specifies the registration, admission, and status protocol. **asn**—(Optional) Displays the output of the decoded protocol data units (PDUs). **event**—(Optional) Displays the events of the H.245 signaling or turns on both traces.
debug npcp [**traces** | **errors** | **np-debug** | **api** | **async** | **gf**] **debug pix** [**process** | **uauth** | **acl** [*limit*] | **cls** | **pkt2pc**]	
debug mgcp [**messages** | **parser** | **sessions**]	Displays Media Gateway Protocol (MGCP) information. **messages**—(Optional) Displays debug information for MGCP messages. **parser**—(Optional) Displays debug information about parsing MGCP messages. **sessions—**(Optional) Displays debug information about sessions.
debug ospf adj | **database-timer** | **events** | **flood** | **lsa-generation** | **packet** | **retransmission** | **tree**	
debug ospf spf [**external** | **inter** | **intra**]	
debug packet *interface_name* [**src** *source_ip* [**netmask** *mask*]] [**dst** *dest_ip* [**netmask** *mask*]] [[**proto tcp** [**sport** *src_port*]] [**dport** *dest_port*] | [**proto udp** [**sport** *src_port*]] [**dport** *dest_port*] [**rx** | **tx** | **both**]	Displays packet information. *interface_name*—Interface name from which the packets are arriving; for example, to monitor packets coming into the FWSM from the outside, set *interface_name* to **outside**. **src** *source_ip*—(Optional) Source IP address. **netmask** *mask*—(Optional) Network mask. **dst** *dest_ip*—(Optional) Destination IP address. **proto tcp**—(Optional) Displays TCP packets only. **sport** *src_port*—(Optional) Source port. See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names. **dport** *dest_port*—(Optional) Destination port. **proto udp**—(Optional) Displays UDP packets only. **rx**—(Optional) Displays only packets that were received at the FWSM. **tx**—(Optional) Displays only packets that were transmitted from the FWSM. **both**—(Optional) Displays packets that were received at or transmitted from the FWSM.

Table 2-7 debug Commands With Arguments or Keywords (continued)

Syntax	Syntax Description
debug pc-lu [**error** | **detail** | **flag**]	
debug radius [**session** | **all** | **user** *username*]	Displays RADIUS information. **session**—(Optional) Logs RADIUS session information and the attributes of sent and received RADIUS packets. **all**—(Optional) Enables all RADIUS debug options. **user** *username*—(Optional) Displays information for an individual *username* only.
debug resmgr [**error** | **all**]	
debug RM-NP-counter clr-all	
debug RM-NP-counter *np vc_id cnt_block cnt_id* [**clr**|**set** *value*]	
debug session [**pscb** | **dt** | **leaf**]	
debug ssl [**cipher** | **device**]	
debug tacacs [*session* | **user** *user_name*]	

Defaults

The defaults are as follows:

- MGCP debugging is disabled.
- A session not using a trace channel has its output disabled.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can set the debugging level with the following commands:

```
fwsm# debug rip 1
debug rip  enabled at level 1
fwsm# debug rip 2
debug rip  enabled at level 2
fwsm# debug rip 3
debug rip  enabled at level 3
fwsm# debug rip 4
debug rip  enabled at level 4
```

```
fwsm# debug rip 100
debug rip  enabled at level 100
fwsm# debug rip 500
debug rip  enabled at level 255
```

Entering the **debug** command allows you to see debug information, and entering the **show debug** command allows you to see the current state of tracing. To debug the contents of network layer protocol packets, use the **debug packet** command.

Note Using the **debug** commands may slow down traffic on busy networks.

If you enter the **debug packet** command on an FWSM that experiences a heavy load, the output might display so fast that you cannot stop the output when you enter the **no debug packet** command from the console. To fix this situation, you can enter the **no debug packet** command from a Telnet session.

To stop the **debug packet trace** command, enter the following command:

```
fwsm/context_name(config)# no debug packet interface_name
```

Replace *interface_name* with the name of the interface; for example, **inside**, **outside**, or a perimeter interface name.

no debug all and undebug all

The **no debug all** and **undebug all** commands allow you to stop any and all debug messages from being displayed.

debug crypto

When creating your digital certificates, use the **debug crypto ca** command to ensure that the certificate is created correctly. Important error messages display only when the **debug crypto ca** command is enabled. For example, if you enter an Entrust fingerprint value incorrectly, the only warning message that indicates that the value is incorrect appears in the **debug crypto ca** command output.

Output from the **debug crypto ipsec** and **debug crypto isakmp** commands does not display in a Telnet console session.

debug dhcpd

The **debug dhcpd detail** command allows you to display detailed packet information about the Dynamic Host Configuration Protocol (DHCP) client. Entering the **debug dhcpd error** command displays DHCP client error messages. Entering the **debug dhcpd packet** command displays packet information about the DHCP client. To disable debugging, use the **no** form of the **debug dhcpd** command.

The **debug dhcpd event** command allows you to display event information about the DHCP server. Entering the **debug dhcpd packet** command displays packet information about the DHCP server. To disable debugging, use the **no** form of the **debug dhcpd** commands.

debug icmp

The **debug icmp trace** command allows you to display ICMP packet information, the source IP address, and the destination address of packets arriving, departing, and traversing the FWSM. This command can trace only packets that are pings to the interfaces.

To stop the **debug icmp trace** command, enter the following command:

```
fwsm/context_name(config)# no debug icmp trace
```

debug mgcp

The **debug mgcp** command allows you to display debug information for Media Gateway Control Protocol (MGCP) traffic. Without any options explicitly specified, the **debug mgcp** command allows you to enable all three MGCP debug options. The **no debug mgcp** command, without any options explicitly specified, disables all MGCP debugging.

debug sqlnet

The **debug sqlnet** command allows you to display reports on traffic between Oracle SQL*Net clients and servers through the FWSM.

debug ssh

The **debug ssh** command allows you to display reports on information and error messages associated with the **ssh** command.

debug fover

Table 2-8 lists the optional keywords for the **debug fover** command.

Table 2-8 debug fover Command Options

Option	Description
cable	Failover LAN status
fail	Failover internal exception
fmsg	Failover message
ifc	Network interface status trace
open	Failover device open
rx	LAN-based failover receive process messages
rxdump	Failover receive message dump (serial console only)
rxip	IP network failover packet received
sync	Failover configuration or command replication
tx	LAN-based failover transmit process messages
txdmp	Failover transmit message dump (serial console only)
txip	IP network failover packet transmit
verify	Failover message verify
switch	Failover switching status

Trace Channel Feature

The **debug packet** command allows you to send its output to the trace channel. All other **debug** commands do not. Using the trace channel changes the way that you can see output on your screen during a FWSM console or Telnet session.

If a **debug** command does not use the trace channel, each session operates independently, which means that any commands started in the session only appear in the session. By default, a session not using a trace channel has output disabled by default.

The location of the trace channel depends on whether you have a simultaneous Telnet console session running at the same time as the console session, or if you are using only the FWSM serial console:

- If you are using only the FWSM serial console, all the **debug** commands display on the serial console.
- If you have both a serial console session and a Telnet console session accessing the console, then no matter where you enter the **debug** commands, the output displays on the Telnet console session.
- If you have two or more Telnet console sessions, the first session is the trace channel. If that session closes, the serial console session becomes the trace channel. The next Telnet console session that accesses the console becomes the trace channel.

The **debug** commands, except the **debug crypto** commands, are shared between all Telnet and serial console sessions.

Caution If one network administrator is using the serial console and another network administrator starts a Telnet console session, the serial console **debug** command output will suddenly stop without warning. If you are using the serial console and **debug** command output is not appearing, enter the **who** command to see if a Telnet console session is running.

Examples

This example shows partial sample output from the **debug dhcpd packet** and the **debug dhcpd detail** commands. The **ip address dhcp setroute** command was configured after entering the **debug dhcpd** commands to obtain debugging information.

```
fwsm/context_name(config)# debug dhcpd packet
fwsm/context_name(config)# debug dhcpd detail
fwsm/context_name(config)# ip address outside dhcp setroute

DHCP:allocate request
DHCP:new entry. add to queue
DHCP:new ip lease str = 0x80ce8a28
DHCP:SDiscover attempt # 1 for entry:
Temp IP addr:0.0.0.0 for peer on Interface:outside
Temp sub net mask:0.0.0.0
   DHCP Lease server:0.0.0.0, state:1 Selecting
   DHCP transaction id:0x8931
   Lease:0 secs, Renewal:0 secs, Rebind:0 secs
   Next timer fires after:2 seconds
   Retry count:1   Client-ID:cisco-0000.0000.0000-outside

DHCP:SDiscover:sending 265 byte length DHCP packet
DHCP:SDiscover 265 bytes
DHCP Broadcast to 255.255.255.255 from 0.0.0.0
DHCP client msg received, fip=10.3.2.2, fport=67
DHCP:Received a BOOTREP pkt
DHCP:Scan:Message type:DHCP Offer
DHCP:Scan:Server ID Option:10.1.1.69 = 450A44AB
DHCP:Scan:Server ID Option:10.1.1.69 = 450A44AB
DHCP:Scan:Lease Time:259200
DHCP:Scan:Subnet Address Option:255.255.254.0
DHCP:Scan:DNS Name Server Option:10.1.1.70, 10.1.1.140
DHCP:Scan:Domain Name:example.com
DHCP:Scan:NBNS Name Server Option:10.1.2.228, 10.1.2.87
DHCP:Scan:Router Address Option:10.3.2.1
DHCP:rcvd pkt source:10.3.2.2, destination: 255.255.255.255
```

This example executes the **debug icmp trace** command:

```
fwsm/context_name(config)# debug icmp trace
```

When you ping a host through the FWSM from any interface, the trace output displays on the console. This example shows a successful ping from an external host (209.165.201.2) to the FWSM outside interface (209.165.201.1).

```
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
NO DEBUG ICMP TRACE
ICMP trace off
```

The previous example shows the Internet Control Message Protocol (ICMP) packet length is 32 bytes, the ICMP packet identifier is 1, and the ICMP sequence number, which starts at 0 and is incremented each time that a request is sent.

The following is sample output from the **show debug** command output. The sample output also includes the **debug crypto** commands.

```
fwsm/context_name(config)# show debug
debug vpdn event
debug crypto ipsec 1
debug crypto isakmp 1
debug crypto ca 1
debug icmp trace
debug packet outside both
debug sqlnet
```

This example shows the debugging messages for Unity client negotiation using Diffie-Hellman group 5:

```
fwsm(config)# debug crypto isakmp

check_isakmp_proposal:
is_auth_policy_configured: auth 1
is_auth_policy_configured: auth 4
ISAKMP (0): Checking ISAKMP transform 1 against priority 8 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 5
ISAKMP:      extended auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 2 against priority 8 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 5
ISAKMP:      extended auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 8 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 5
ISAKMP:      auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are not acceptable. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 4 against priority 8 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 5
```

```
ISAKMP:      auth RSA sig
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x20 0xc4 0x9b
ISAKMP (0): atts are acceptable. Next payload is 3
```

This example shows possible output for the **debug mgcp messages** command:

```
17: MGCP: Retransmitted command RSIP
        Gateway IP      gate-1
        Transaction ID  1
18: MGCP: Expired command RSIP
        Gateway IP      gate-1
        Transaction ID  1
19: MGCP: New command RSIP
        Gateway IP      gate-1
        Transaction ID  1
        Endpoint name   d001
        Call ID
        Connection ID
        Media IP        0.0.0.0
        Media port      0
        Flags           0x80
20: MGCP: Retransmitted command RSIP
        Gateway IP      gate-1
        Transaction ID  1
```

This example shows possible output for the **debug mgcp parser** command:

```
28: MGCP packet:
RSIP 1 d001@10.10.10.11 MGCP 1.0
RM: restart

29: MGCP: command verb - RSIP
30: MGCP: transaction ID - 1
31: MGCP: endpoint name - d001
32: MGCP: header parsing succeeded
33: MGCP: restart method - restart
34: MGCP: payload parsing succeeded
35: MGCP packet:
RSIP 1 d001@10.10.10.11 MGCP 1.0
RM: restart

36: MGCP: command verb - RSIP
37: MGCP: transaction ID - 1
38: MGCP: endpoint name - d001
39: MGCP: header parsing succeeded
40: MGCP: restart method - restart
41: MGCP: payload parsing succeeded
```

This example shows possible output for the **debug mgcp sessions** command:

```
91: NAT::requesting UDP conn for generic-pc-2/6166 [192.168.5.7/0]
        from dmz/ca:generic-pc-2/2427 to outside:generic-pc-1/2727
92: NAT::reverse route: embedded host at dmz/ca:generic-pc-2/6166
93: NAT::table route: embedded host at outside:192.168.5.7/0
94: NAT::pre-allocate connection for outside:192.168.5.7 to dmz/ca:generic-pc-2/6166
95: NAT::found inside xlate from dmz/ca:generic-pc-2/0 to outside:172.23.58.115/0
96: NAT::outside NAT not needed
97: NAT::created UDP conn dmz/ca:generic-pc-2/6166 <-> outside:192.168.5.7/0
98: NAT::created RTCP conn dmz/ca:generic-pc-2/6167 <-> outside:192.168.5.7/0
99: NAT::requesting UDP conn for 192.168.5.7/6058 [generic-pc-2/0]
        from dmz/ca:genericgeneric-pc-2/2427 to outside:generic-pc-1/2727
100: NAT::table route: embedded host at outside:192.168.5.7/6058
101: NAT::reverse route: embedded host at dmz/ca:generic-pc-2/0
```

```
102: NAT::pre-allocate connection for dmz/ca:generic-pc-2 to outside:192.168.5.7/6058
103: NAT::found inside xlate from dmz/ca:generic-pc-2/0 to outside:172.23.58.115/0
104: NAT::outside NAT not needed
105: NAT::created UDP conn dmz/ca:generic-pc-2/0 <-> outside:192.168.5.7/6058
106: NAT::created RTCP conn dmz/ca:generic-pc-2/0 <-> outside:192.168.5.7/6059
107: MGCP: New session
        Gateway IP     generic-pc-2
        Call ID        9876543210abcdef
        Connection ID  6789af54c9
        Endpoint name  aaln/1
        Media lcl port 6166
        Media rmt IP   192.168.5.7
        Media rmt port 6058
108: MGCP: Expired session, active 0:06:05
        Gateway IP      generic-pc-2
        Call ID         9876543210abcdef
        Connection ID   6789af54c9
        Endpoint name   aaln/1
        Media lcl port  6166
        Media rmt IP    192.168.5.7
        Media rmt port  6058
```

This example shows how to debug the contents of packets with the **debug packet** command:

```
fwsm/context_name(config)# debug packet inside
--------- PACKET ---------
-- IP --
4.3.2.1 ==>     255.3.2.1
        ver = 0x4       hlen = 0x5      tos = 0x0       tlen = 0x60
        id = 0x3902     flags = 0x0     frag off=0x0
        ttl = 0x20      proto=0x11      chksum = 0x5885
        -- UDP --
                source port = 0x89      dest port = 0x89
                len = 0x4c      checksum = 0xa6a0
        -- DATA --
                00000014:                                       00 01 00 00  |
         ....
                00000024: 00 00 00 01 20 45 49 45 50 45 47 45 47 45 46 46  | ..
.. EIEPEGEGEFF
                00000034: 43 43 4e 46 41 45 44 43 41 43 41 43 41 43 41 43  | CC
NFAEDCACACACAC
                00000044: 41 43 41 41 41 00 00 20 00 01 c0 0c 00 20 00 01  | AC
AAA.. ..... ..
                00000054: 00 04 93 e0 00 06 60 00 01 02 03 04 00          | ..
....`......
--------- END OF PACKET ---------
```

This example shows sample output from the **show debug** command:

```
fwsm/context_name(config)# show debug
debug icmp trace off
debug packet off
debug sqlnet off
```

Related Commands

mgcp
show conn
timeout

default-information originate (router OSPF subcommand)

To generate a type 7 default in the not-so-stubby area (NSSA), use the **default-information originate** command.

default-information originate [**always**] [**metric** *metric_value*] [**metric-type** {**1** | **2**}] [**route-map** *map_name*]

Syntax Description

always	(Optional) Specifies that a type 7 default is always generated.
metric *metric_value*	(Optional) Specifies the Open Shortest Path First (OSPF) default metric value from 0 to 16777214.
metric-type 1	(Optional) Specifies the type of OSPF metric routes; valid values are **1**.
metric-type 2	(Optional) Specifies the type of OSPF metric routes; valid values are **2**.
route-map *map_name*	(Optional) Name of the route map to apply.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is supported on an NSSA area border router (ABR) or an NSSA autonomous system boundary router (ASBR) only.

The **show router ospf** command displays the configured **router ospf** subcommands.

Examples

This example shows how to configure router ospf:

```
fwsm(config)# router ospf 1
fwsm(config-router)# default-information originate metric 5
fwsm(config-router)#
```

This example shows how to disply the configured router ospf subcommands:

```
fwsm(config)# show router ospf
!
router ospf 1
        network 10.1.1.0 255.255.255.0 area 0
        log-adj-changes
        default-information originate metric 5
```

Related Commands

router ospf
show default-information originate
show ip ospf
show router ospf

delete

To delete a file in the disk partition, use the **delete** command.

delete[**/recursive**] [**/force**] [**/noconfirm**] [**disk:**]*path*

Syntax Description

/recursive	(Optional) Deletes the specified file recursively in all subdirectories.
/force	(Optional) Deletes the specified file without prompting you to confirm the delete action.
/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	(Optional) Changes the current working directory.
path	Specifies the path and filename.

Defaults

If you do not specify a directory, the directory is **disk:** by default.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The filename prompt is still on if the disk partition is the only option. However, you may include it before the path.

The file is deleted from the current working directory if a path is not specified. Wildcards are supported when deleting files. When deleting files, you are prompted with the filename and you must confirm the delete. If you use the **delete disk** command, you are prompted to enter the filename for deletion.

Examples

This example shows how to delete a file named test.cfg in the root directory:

```
fwsm(config)# delete test.cfg
```

This example shows how to recursively delete all files but not directories under the configuration directory:

```
fwsm(config)# delete /recursive disk:/configs/*
```

All files in the disk partition are deleted because of the wildcard * meaning all.

This example shows how to force a file deletion:

```
fwsm(config)# delete /force *
```

Related Commands

cd
copy disk
copy flash
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir
show file

description (submode)

To configure the context description information, use the **description** command. To remove the context description information from the configuration, use the **no** form of this command.

[**no**] **description** *text*

Syntax Description

text	Context description.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **description** command can also be used as a context submode command and an object-group submode command.

Examples

This example shows how to configure the context description information:

```
fwsm(config)# context my-context
Creating context 'my-context'... Done. (2) FWSM(config-context)# description my admin
context fwsm(config-context)# show context detail
Context "admin", is ADMIN and active
  Config URL: disk:/admin.cfg
  Real Interfaces: vlan2, vlan100-101
  Mapped Interfaces: vlan2, vlan100-101
  Class: default, Flags: 0x00001857, ID: 1

Context "my-context", has been created, but not initialized
  Desc: my admin context
  Config URL: n/a
  Real Interfaces:
  Mapped Interfaces:
  Class: default, Flags: 0x00000801, ID: 2

Context "system", is a system resource
  Config URL: flash:config
  Real Interfaces:
  Mapped Interfaces: eobc, vlan2, vlan100-101
  Class: default, Flags: 0x00000019, ID: 257
```

```
Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Class: default, Flags: 0x00000009, ID: 258 FWSM(config-context)#
```

Related Commands

context

dhcpd

To configure the DHCP server, use the **dhcpd** command. To remove the specified configuration or disable a function, use the **no** form of this command.

dhcpd {**address** *ip1*[**-***ip2*] *srv_interface_name*} | {**dns** *dnsip1* [*dnsip2*]} | {**wins** *winsip1* [*winsip2*]} | {**lease** *lease_length*} | {**domain** *domain_name*} | {**enable** *srv_interface_name*}

dhcpd {**option** *code ascii string* | **hex** *hex_string* | {**ip** *address_1* | *address_2*]}

dhcpd ping_timeout *timeout*

no dhcpd option *code*

Syntax Description

address *ip1*	Start address of the DHCP address pool.
address *ip2*	(Optional) End address of the DHCP address pool.
srv_interface_name	Interface to enable DHCP server.
dns *dnsip1*	IP addresses of the DNS servers for the DHCP client.
dns *dnsip2*	(Optional) IP addresses of the DNS servers for the DHCP client.
wins *winsip1*	Specifies the IP addresses of the Microsoft NetBIOS name servers (WINS server).
wins *winsip2*	(Optional) Specifies the IP addresses of the Microsoft NetBIOS name servers (WINS server).
lease *lease_length*	Specifies the length of the lease, in seconds, granted to the DHCP client from the DHCP server; valid values are from 300 to 1048575 seconds.
domain *domain_name*	Specifies the DNS domain name.
enable *server_interface_name*	Specifies the interface on which to enable the DHCP server.
option *code*	Specifies the positive number representing the DHCP option code; valid values are **66** or **150**.
ascii string	ASCII character string without white space representing the TFTP server.
hex *hex_string*	Specifies the TFTP server in dotted decimal format, such as 1.1.1.1, but is treated as a character string without white spaces by the FWSM DHCP server.
ip *address_1*	Specifies the IP addresses of a TFTP server.
ip *address_2*	(Optional) Specifies the IP addresses of a TFTP server.
ping_timeout *timeout*	Allows the configuration of the timeout value of a ping in milliseconds, before assigning an IP address to a DHCP client.

Defaults

lease_length is 3600 seconds.
ping_timeout *timeout* is 50 seconds.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **address** *ip1* [*ip2*] allows you to specify an IP pool address range.

If the address pool range is larger than 253 addresses, the netmask of the FWSM interface cannot be a Class C address (for example, 255.255.255.0) and needs to be something larger, for example, 255.255.254.0.

The **dns** *dns1* [*dns2*] command allows you to specify that the DNS A (address) resource records that match the static translation are rewritten. A second server address is optional.

The **lease** *lease_length* command allows you to configure the length of the lease, in seconds, that are granted to the DHCP client from the DHCP server. The lease indicates how long the client can use the assigned IP address. The default is 3600 seconds. The minimum lease length is 300 seconds, and the maximum lease length is 2,147,483,647 seconds.

The **option 150** command allows you to specify the TFTP server IP address(es) that are designated for Cisco IP phones in dotted decimal format. DHCP option 150 is site specific; it gives the IP addresses of a list of TFTP servers.

A DHCP server provides network configuration parameters to a DHCP client. Support for the DHCP server within the FWSM means that the FWSM can use DHCP to configure connected clients. This DHCP feature is designed for the remote home or branch office that will establish a connection to an enterprise or corporate network. Refer to the *Cisco Firewall and VPN Configuration Guide* for information on how to implement the DHCP server feature into the FWSM.

You must specify an interface name, *interface_name*, for the **dhcpd address** and **dhcpd enable** commands when using FWSM software Version 2.2(1). In earlier software versions, only the inside interface could be configured as the DHCP server so there was no need to specify *interface_name*.

Note The FWSM DHCP server does not support some BOOTP requests or failover configurations.

The **dhcpd address** *ip1*[**-***ip2*] *interface_name* command allows you to specify the DHCP server address pool. The address pool of a FWSM DHCP server must be within the same subnet of the FWSM interface that is enabled, and you must specify the associated FWSM interface with the *interface_name*. The client must be physically connected to the subnet of a FWSM interface. The size of the pool is limited to 256 per pool on the FWSM. The unlimited user license on the FWSM and all other FWSM platforms support 256 addresses. The **dhcpd address** command cannot use names with a "-" (dash) character because the "-" character is interpreted as a range specifier instead of as part of the object name.

The **no dhcpd address** command allows you to remove the DHCP server address pool that you configured.

The **dhcpd dns** command allows you to specify the IP address(es) of the DNS server(s) for the DHCP client. You can specify two DNS servers. The **no dhcpd dns** command allows you to remove the DNS IP address(es) from the configuration.

The **dhcpd wins** command allows you to specify the addresses of the WINS server for the DHCP client. The **no dhcpd dns** command allows you to remove the WINS server IP address(es) from the configuration.

The **dhcpd lease** command allows you to specify the length of the lease in seconds that are granted to the DHCP client. This lease indicates how long the DHCP client can use the assigned IP address that the DHCP granted. The **no dhcpd lease** command allows you to remove the lease length that you specified from the configuration and replaces this value with the default value of 1048575 seconds.

The **dhcpd domain** command allows you to specify the DNS domain name for the DHCP client. The **no dhcpd domain** command allows you to remove the DNS domain server from the configuration.

The **dhcpd enable** *interface_name* command allows you to enable the DHCP daemon to listen for the DHCP client requests on the DHCP-enabled interface. The **no dhcpd enable** command disables the DHCP server feature on the specified interface.

You must enable DHCP to use this command. Use the **dhcpd enable** *interface_name* command to turn on DHCP.

Note The FWSM DHCP server daemon does not support clients that are not directly connected to a FWSM interface.

The **dhcpd option 66 | 150** command allows you to retrieve TFTP server address information for IP phone connections.

When a **dhcpd option** command request arrives at the FWSM DHCP server, the FWSM places the value(s) that are specified by the **dhcpd option 66 | 150** in the response.

Use the **dhcpd option** *code* command as follows:

- If the TFTP server for IP phone connections is located on the inside interface, use the local IP address of the TFTP server in the **dhcpd option** command.
- If the TFTP server is located on a less secure interface, create a group of NAT global and access-list entries for the inside IP phones, and use the actual IP address of the TFTP server in the **dhcpd option** command.
- If the TFTP server is located on a more secure interface, create a group of static and access-list statements for the TFTP server and use the global IP address of the TFTP server in the **dhcpd option** command.

The **debug dhcpd event** command allows you to display event information about the DHCP server. The **debug dhcpd packet** command displays packet information about the DHCP server. To disable debugging, use the **no** form of the **debug dhcpd** commands.

Examples

This partial example shows how to use the **dhcpd address**, **dhcpd dns**, and **dhcpd enable** *interface_name* commands to configure an address pool for the DHCP clients and a DNS server address for the DHCP client, and how to enable the **dmz** interface of the FWSM for the DHCP server function.

```
fwsm/context_name(config)# ip address dmz 10.0.1.1 255.255.0.0
fwsm/context_name(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
fwsm/context_name(config)# dhcpd dns 209.165.200.226
fwsm/context_name(config)# dhcpd enable dmz
```

This partial example shows how to use three new features that are associated with each other: DHCP server, and PAT using interface IP to configure a FWSM in a small office and home office (SOHO) environment with the **inside** interface as the DHCP server:

```
! enable dhcp server daemon on the inside interface
fwsm/context_name(config)# ip address inside 10.0.1.2 255.255.255.0
fwsm/context_name(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
fwsm/context_name(config)# dhcpd dns 209.165.201.2 209.165.202.129
fwsm/context_name(config)# dhcpd wins 209.165.201.5
fwsm/context_name(config)# dhcpd lease 3000
fwsm/context_name(config)# dhcpd domain example.com
fwsm/context_name(config)# dhcpd enable inside
! use outside interface IP as PAT global address
fwsm/context_name(config)# nat (inside) 1 0 0
fwsm/context_name(config)# global (outside) 1 interface
```

This example shows sample output from the **show dhcpd** command:

```
fwsm/context_name(config)# show dhcpd
dhcpd address 10.0.1.100-10.0.1.108 dmz
dhcpd dns 192.23.21.23
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable dmz
```

This example shows sample output from the **show dhcpd binding** command:

```
fwsm/context_name(config)# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

This example shows sample output from the **show dhcpd statistics** command:

```
fwsm/context_name(config)# show dhcpd statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        2
Automatic bindings   0
Expired bindings     0
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0
```

```
Message              Sent
BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
```

Related Commands

clear dhcpd
dhcprelay
ip address
show dhcpd
show dhcprelay

dhcprelay

To configure the DHCP relay agent, which relays requests between the FWSM interface of the DCHP server and DHCP clients on a different FWSM interface, use the **dhcprelay** command. To remove the DHCP relay agent configuration, use the **no** form of this command.

[**no**] **dhcprelay enable** *client_interface*

[**no**] **dhcprelay server** *server_ip server_interface*

[**no**] **dhcprelay setroute** *client_interface*

[**no**] **dhcprelay timeout** *seconds*

Syntax Description

enable	Enables the DHCP relay agent to accept DHCP requests from clients on the specified interface.
client_interface	Name of the interface on which the DHCP relay agent accepts client requests.
server *server_ip*	IP address of the DHCP server to which the DHCP relay agent forwards client requests.
server_interface	Name of the FWSM interface on which the DHCP server resides.
setroute *client_interface*	Configures the DHCP relay agent to change the first default router address (in the packet sent from the DHCP server) to the address of *client_interface*.
timeout *seconds*	Specifies the number of seconds that are allowed for DHCP relay address negotiation.

Defaults

The defaults are as follows:

- DHCP relay agent is disabled.
- *seconds* is 60 seconds.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

In order for the FWSM to start the DHCP relay agent with the **dhcprelay enable** *client_interface* command, you must have a **dhcprelay server** command already in the configuration. Otherwise, the FWSM displays an error message similar to the following:

```
DHCPRA:Warning - There are no DHCP servers configured!
       No relaying can be done without a server!
       Use the 'dhcprelay server <server_ip> <server_interface>' command
```

The **dhcprelay enable** *client_interface* command allows you to start a DHCP server task on the specified interface. If this **dhcprelay enable** command is the first **dhcprelay enable** command to be entered, and there are **dhcprelay server** commands in the configuration, then the ports for the DHCP servers referenced are opened and the DHCP relay task starts.

dhcprelay server

Add at least one **dhcprelay server** command to the FWSM configuration before you enter the **dhcprelay enable** command or the FWSM will display an error message.

The **dhcprelay server** command allows you to open a UDP port 67 on the specified interface for the specified server and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration. If there is **no dhcprelay enable** command in the configuration, then the sockets are not opened and the DHCP relay task does not start.

When you remove the **dhcprelay server** *dhcp_server_ip* [*server_interface*] command, the port for that server is closed. If the **dhcprelay server** command being removed is the last **dhcprelay server** command in the configuration, then the DHCP relay task stops.

dhcprelay setroute

The **dhcprelay setroute** *client_interface* command allows you to enable the DHCP relay agent to change the first default router address (in the packet sent from the DHCP server) to the address of *client_interface*. The DHCP relay agent substitutes the address of the default router with the address of *client_interface*.

If there is no default router option in the packet, the FWSM adds one containing the address of *client_interface*. This action allows the client to set its default route to point to the FWSM.

When you do not configure the **dhcprelay setroute** *client_interface* command (and there is a default router option in the packet), it passes through the FWSM with the router address unaltered.

dhcprelay timeout

The **dhcprelay timeout** command allows you to set the amount of time, in seconds, allowed for responses from the DHCP server to pass to the DHCP client through the relay binding structure.

no dhcprelay commands

The **no dhcprelay enable** *client_interface* command allows you to remove the DHCP relay agent configuration for the interface that is specified by *client_interface* only.

The **no dhcprelay server** *dhcp_server_ip* [*server_interface*] command allows you to remove the DHCP relay agent configuration for the DHCP server that is specified by *dhcp_server_ip* [*server_interface*] only.

Examples

This example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the FWSM, client requests on the inside interface of the FWSM, and a timeout value up to 60 seconds:

```
fwsm(config)# dhcprelay server 10.1.1.1 outside
fwsm(config)# dhcprelay timeout 60
fwsm(config)# dhcprelay enable inside
fwsm(config)# show dhcprelay
dhcprelay server 10.1.1.1 outside dhcprelay enable inside dhcprelay timeout 60
fwsm(config)#
```

This example shows how to disable the DHCP relay agent if there is only one **dhcprelay enable** command in the configuration:

```
fwsm(config)# no dhcprelay enable inside
fwsm(config)# show dhcprelay
dhcprelay server 10.1.1.1 outside dhcprelay timeout 60
fwsm(config)#
```

This example shows the output of the **show dhcprelay statistics** command:

```
fwsm/context_name(config)# show dhcprelay statistics
DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         0
DHCPREQUEST          0
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            0
DHCPACK              0
DHCPNAK              0
```

Related Commands

clear dhcprelay
dhcpd
show dhcpd
show dhcprelay

dir

To display the directory contents, use the **dir** command.

dir [**/recursive**] [**disk:**] [**flash:**][*path*]

Syntax Description

/recursive	(Optional) Displays the directory contents recursively.
disk:	(Optional) Specifies the disk file system.
flash:	(Optional) Displays the contents of the default Flash partition.
path	(Optional) Path for the directory.

Defaults

If you do not specify a directory, the directory is changed to **disk:** by default.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **dir** command without keyword or arguments displays the directory contents of the current directory.

Examples

This example shows how to display the directory contents:

```
fwsm(config)# dir
Directory of disk:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

This example shows how to display recursively the contents of the disk:

```
fwsm(config)# dir /recursive disk:
Directory of disk:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

This example shows how display the contents of the Flash partition:

```
fwsm(config)# dir flash:
Directory of flash:/
0      -wx  6783044    <no date>  image
1      rw-  1314       <no date>  startup-config
```

Related Commands

cd
copy disk
copy flash
copy tftp
format
mkdir
more
pwd
rename
rmdir
show file

disable

To exit privileged mode and return to unprivileged mode, use the **disable** command.

disable

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use the **enable** command to enter privileged mode. The **disable** command allows you to exit privileged mode and returns you to unprivileged mode.

Examples

This example shows how to enter privileged mode:

```
fwsm> enable
fwsm#
```

This example shows how to exit privileged mode:

```
fwsm# disable
fwsm>
```

distance (router submode)

To define Open Shortest Path First (OSPF) route administrative distances that are based on route type, use the **distance** command. To return to the default setting, use the **no** form of this command.

distance ospf [**intra-area** *d1*][**inter-area** *d2*][**external** *d3*]

no distance ospf

Syntax Description

intra-area	(Optional) Sets the distance for all routes within an area.
d1, *d2*, and *d3*	(Optional) Distance for different area route types.
inter-area	(Optional) Sets the distance for all routes from one area to another area.
external	(Optional) Sets the distance for routes from other routing domains that are learned by redistribution.

Defaults

d1, *d2*, and *d3* 110.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show ip ospf** command displays general information about the OSPF routing processes.

Examples

This example shows how to define an OSPF route administrative distance:

```
fwsm(config)# router ospf 1
fwsm(config-router)# distance intra-area 100 inter-area 120 external 150
fwsm(config-router)#
```

Related Commands

router ospf
show distance
show ip ospf
show router ospf

domain-name

To change the domain name, use the **domain-name** command. To remove the domain name, use the **no** form of this command.

[**no**] **domain-name** *name*

Syntax Description

name	A domain name that is less than 63 characters.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **domain-name** command allows you to change the domain name.

Note This command sets the domain name to a fully qualified domain name. The RSA key uses this domain name and you must use the host name. If you change the domain name, you need to redo the RSA keys.

Examples

This example shows how to use the **domain-name** command:

```
fwsm/context_name(config)# domain-name example.com
```

or

```
FWSM(config)# domain-name 12345678901234567890123456789012345678901234567890123$
Domain name must be less than 63 characters.
FWSM(config)# domain-name 1234567890123456789012345678901234567890123456789012$
FWSM(config)#
```

Related Commands

show domain-name

dynamic-map

To create a dynamic crypto map entry template, use the **dynamic-map** command.

dynamic-map *map seq subcommand*

Syntax Description

map	Dynamic crypto map template tag.
seq	Sequence number to insert into the dynamic crypto map entry.
subcommand	Subcommands; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear dynamic-map** command allows you to remove the **dynamic-map** commands from the configuration. The **show dynamic-map** command allows you to display the **dynamic-map** commands in the configuration.

Note The **dynamic-map** command is the same as the **crypto dynamic-map** command. Refer to the **crypto dynamic-map** command for more information.

Examples

This example shows how to create a dynamic crypto map entry:

```
fwsm/context_name(config)# dynamic-map test 10 match address test-acl
```

Related Commands

show dynamic-map

enable

To access privileged mode or privilege levels, or to set the enable password, use the **enable** command. Use the **no** form of this command to change the password.

[**no**] **enable** [*pw*] [**level** *level*] [**encrypted**]

Syntax Description

pw	(Optional) Password for this privilege level. The minimum is three characters.
level	(Optional) Privilege level, from 0 to 15.
encrypted	(Optional) Specifies that the provided password is already encrypted.

Defaults

The privilege *level* is 15.

The password is blank.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode to set the password

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **enable** command allows you to enter privileged mode. The FWSM prompts you for your privileged mode password. By default, the enable password is blank—you can press the **Enter** key at the password prompt to start privileged mode. Use the **disable** command to exit privileged mode. Use the **enable password** command to change the password.

If you do not enter a level, the level is 15. If you enter a level, you are prompted for the password set for that level. If you configure local command authorization with the **aaa authorization** command, and you set command privilege levels (**privilege** command), you can only use commands available at that level. If no command authorization is used, then level 2 and above is privileged mode and you can access all privileged commands.

Note If you define privilege levels 10 and 12, the level 15 password is not changed or removed.

The **enable password** command allows you to change the privileged mode password. The FWSM prompts you for the privileged mode password after you enter the **enable** command. You can return the enable password to its original value (press the **Enter** key at the prompt) by entering the **no enable password** command.

The **encrypted** keyword appears in the configuration when you set the password. You cannot see the original password in the configuration, you can see only the encrypted form. Copy the configuration passwords to another FWSM in their encrypted form by cutting and pasting the **enable** command including the encryped argument.

Examples

This example shows how to enter privileged mode with the **enable** command and then enter configuration mode with the **configure terminal** command:

```
fwsm> enable
Password:
fwsm# configure terminal
fwsm(config)#
```

This example shows how to enter privileged mode with the **enable** command, change the enable password with the **enable password** command, enter configuration mode with the **configure terminal** command, and display the contents of the current configuration with the **write terminal** command:

```
fwsm> enable
Password:
fwsm# enable password w0ttal1fe
fwsm# configure terminal
fwsm(config)# write terminal
Building configuration...
enable password 2oifudsaoid.9ff encrypted
```

This example shows how to encrypt your password:

```
fwsm# enable password 1234567890123456 encrypted
fwsm# show enable password
enable password 1234567890123456 encrypted

fwsm# enable password 1234567890123456
fwsm# show enable password
enable password feCkwUGktTCAgIbD encrypted
```

This example shows how to set enable passwords for each level:

```
fwsm(config)# enable password cisco level 10
fwsm(config)# show enable
enable password wC38a.EQklqK3ZqY level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted

fwsm(config)# enable password wC38a.EQklqK3ZqY level 12 encrypted
fwsm(config)# show enable
enable password wC38a.EQklqK3ZqY level 10 encrypted
enable password wC38a.EQklqK3ZqY level 12 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted

fwsm(config)# no enable password level 12
fwsm(config)# show enable
enable password wC38a.EQklqK3ZqY level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted

fwsm(config)# no enable password level 10
fwsm(config)# show enable
enable password 8Ry2YjIyt7RRXU24 encrypted
```

Related Commands

show enable

established

To permit return connections on ports that are based on an established connection, use the **established** command. To disable the **established** feature, use the **no** form of this command.

[**no**] **established** *est_protocol dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

Syntax Description

protocol	IP protocol (UDP or TCP) to use for the established connection lookup.
dport	Destination port to use for the established connection lookup.
sport	(Optional) Source port to use for the established connection lookup.
permitto	(Optional) Allows the return protocol connections destined to the specified port.
protocol	IP protocol (UDP or TCP) used by the return connection.
port -port	UDP or TCP destination port of the return connection.
permitfrom	Allows the return protocol connection(s) originating from the specified port.

Defaults

The defaults are as follows:

- *dport*—0 (wildcard)
- *sport*—0 (wildcard)

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **established** command allows you to permit return access for outbound connections through the FWSM. This command works with an original connection that is outbound from a network and protected by the FWSM and a return connection that is inbound between the same two devices on an external host. The **established** command allows you to specify the destination port that is used for connection lookups. This addition allows more control over the command and provides support for protocols where the destination port is known, but the source port is not. The **permitto** and **permitfrom** keywords refine the return inbound connection.

Caution We recommend that you always specify the **established** command with the **permitto** and **permitfrom** keywords. Using the **established** command without these keywords is a security risk because when connections are made to external systems, those system can make unrestricted connections to the internal host involved in the connection. This situation can be exploited for an attack of your internal systems.

The following potential security violations could occur if you do not use the **established** command correctly.

This example shows that if an internal system makes a TCP connection to an external host on port 4000, then the external host could come back in on any port using any protocol:

```
fwsm/context_name(config)# established tcp 0 4000
```

This example shows that the *src_port* is the originating traffic's source port. You can specify it as 0 if the protocol does not specify which source ports are used. The *dest_port* is the originating traffic's destination port. You can specify it as **0** if the protocol does not specify which destination ports are used. Use wildcard ports (0) only when necessary.

```
fwsm/context_name(config)# established tcp 0 0
```

Note To allow the **established** command to work properly, the client must listen on the port that is specified with the **permitto** keyword.

You can use the **established** command with the **nat 0** command (where there are no **global** commands).

Note You cannot use the **established** command with Port Address Translation (PAT).

The FWSM supports XDMCP (X Display Manager Control Protocol) with assistance from the **established** command.

Caution Using XWindows system applications through the FWSM may cause security risks.

XDMCP is on by default, but it does not complete the session unless you enter the **established** command as follows:

```
fwsm/context_name(config)# established tcp 0 6000 to tcp 6000 from tcp 1024-65535
```

Entering the **established** command enables the internal XDMCP-equipped (UNIX or ReflectionX) hosts to access external XDMCP-equipped XWindows servers. UDP/177-based XDMCP negotiates a TCP-based XWindows session, and subsequent TCP back connections are permitted. Because the source port(s) of the return traffic is unknown, specify the *sport* field as 0 (wildcard). The *dport* should be 6000 + *n*, where *n* represents the local display number. Use this UNIX command to change this value:

```
fwsm/context_name(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

The **established** command is needed because many TCP connections are generated (based on user interaction) and the source port for these connections is unknown. Only the destination port is static. The FWSM does XDMCP fixups transparently. No configuration is required, but you must enter the **established** command to accommodate the TCP session.

Examples

This example shows a connection between two hosts using protocol A from the SRC port B destined for port C. To permit return connections through the FWSM and protocol D (protocol D can be different from protocol A), the source port(s) must correspond to port F and the destination port(s) must correspond to port E.

```
fwsm/context_name(config)# established A B C permitto D E permitfrom D F
```

This example shows how a connection is started by an internal host to an external host using TCP source port 6060 and any destination port. The FWSM permits return traffic between the hosts through TCP destination port 6061 and TCP source port 6059.

```
fwsm/context_name(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 6059
```

This example shows how a connection is started by an internal host to an external host using UDP destination port 6060 and any source port. The FWSM permits return traffic between the hosts through TCP destination port 6061 and TCP source port 1024-65535.

```
fwsm/context_name(config)# established udp 0 6060 permitto tcp 6061 permitfrom tcp
1024-65535
```

This example shows how a local host 10.1.1.1 starts a TCP connection on port 9999 to a foreign host 209.165.201.1. The example allows packets from the foreign host 209.165.201.1 on port 4242 back to local host 10.1.1.1 on port 5454.

```
fwsm/context_name(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

This example shows how to allow packets from foreign host 209.165.201.1 on any port back to local host 10.1.1.1 on port 5454:

```
fwsm/context_name(config)# established tcp 9999 permitto tcp 5454
```

Related Commands

clear established
show established

exit

To exit an access mode, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode and Configuration

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use the **exit** command to exit an access mode. This command has the same function as the **quit** command.

You may also use the key sequence **Ctrl–Z** to exit.

Examples

This example shows how to exit configuration mode and privileged mode:

```
fwsm(config)# exit
fwsm# exit
fwsm>
```

Related Commands

quit

failover

To enable failover on a standby FWSM, use the **failover** command. To disable the failover configuration, use the **no** form of this command.

[**no**] **failover**

[**no**] **failover** [**active**]

Syntax Description

active	(Optional) Makes the FWSM the active module in a failover pair.

Defaults

Disabled

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The failover feature provides high availability for the FWSM. You can install up to four FWSMs in a single switch chassis, and you can designate a pair of modules for a failover with two FWSMs working together as active and standby modules. Inter- and intrachassis topologies are supported.

Note The failover pair must be two otherwise identical modules with compatible FWSM hardware and software.

The **no** form of this command switches the module to standby. The failover feature supports stateful failover or logical updates.

Use the **failover active** command to initiate a failover switch from the standby module, or use the **no failover active** command from the active module to initiate a failover switch. You can use this feature to return a failed module to service, or to force an active module offline for maintenance. Because the standby module does not keep state information on each connection, all active connections are dropped and must be reestablished by the clients.

You can see the information from the **show failover** command using SNMP.

You can monitor 250 interfaces for failover.

You can see the IP addresses of the standby module with the **show ip address** command. The current IP addresses are the same as the system IP addresses on the failover active module except for the failover interface. The system IP addresses will always be those addresses that are configured for the primary module. The current IP addresses will either be those addresses that are configured for the primary or the secondary module, depending on whether the module is the active or the standby module.

Use the IP address from the **ip address** *ip_address* with the **ping** command to check the status of the standby module. This address must be on the same network as the system IP address. For example, if the system IP address is 192.159.1.3, set the failover IP address to 192.159.1.4.

The interface name of a VLAN logical interface cannot be used for *interface_name*.

Examples

When properly configured, the failover configurations for your primary and secondary FWSMs must be different and must reflect which is the primary FWSM and which is the secondary FWSM.

This example shows how to configure the primary FWSM:

```
fwsm(config)# failover lan unit primary
fwsm(config)# failover lan interface lanlink vlan 9
fwsm(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby 172.27.48.2
fwsm(config)# failover
```

This example shows how to configure the secondary FWSM:

```
fwsm(config)# failover lan unit secondary
fwsm(config)# failover lan interface lanlink vlan 9
fwsm(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby 172.27.48.2
fwsm(config)# failover
```

Related Commands

clear failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

failover interface ip

To specify the IP address and mask for the failover or stateful interface and the failover peer interface, use the **failover interface ip** command.

failover interface ip *interface_name ip_address mask* **standby** *ip_address*

Syntax Description

interface_name	Interface name for the failover or stateful interface.
ip_address mask	IP address for the failover or stateful interface on the active module.
standby *ip_address*	Specifies the IP address used by the standby module to communicate with the active module.

Defaults

Not configured

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Failover and stateful interfaces are functions of Layer 3, even when they are in transparent firewall mode and are global to the system. You configure failover in the system context mode (except for the **monitor-interface** command).

Examples

This example shows how to specify the IP address and mask for the failover interface:

```
fwsm(config)# failover lan interface lanlink vlan 9
fwsm(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby 172.27.48.2
FAILOVER INTERFACE-POLICY
```

or

```
fwsm(config)# failover interface-policy 20%
```

Related Commands

clear failover
failover
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

failover interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **failover interface-policy** command. To restore the default, use the **no** form of this command.

failover interface-policy *n*[**%**]

Syntax Description

n	Number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces.
%	(Optional) Specifies that the number *n* is a percentage of the monitored interfaces.

Defaults

50 percent

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

There is no space between the *n* argument and the optional **%** keyword.

Note The keyword percent is still supported for backward compatibility.

If the number of failed interfaces meets the configured policy and the other FWSM is functioning properly, the FWSM will mark itself as failed and a failover may occur (if the active FWSM is the one that fails).

Examples

These examples show two ways to specify the failover policy:

```
fwsm(config)# failover interface-policy 20 percent

fwsm(config)# failover interface-policy 5
```

Related Commands

clear failover
failover
failover interface ip
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

failover lan interface

To specify the interface name and VLAN used for failover communication, use the **failover lan interface** command. To remove the failover interface, use the **no** form of this command.

[**no**] **failover lan interface** *interface_name* **vlan** *vlan*

Syntax Description

interface_name	Name of the FWSM interface that is dedicated to the failover.
vlan *vlan*	Sets the VLAN number.

Defaults

Not configured

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The active and standby modules constantly communicate over this link to determine the operating status of each module. Communications over the failover link include the the module state (active or standby), hello messages (also sent on all other interfaces), and configuration synchronization between the two modules.

A failover requires a dedicated interface, but you can use the same interface for a stateful failover. The interface needs enough capacity to handle both the LAN-based failover and stateful failover traffic.

Note We recommend that you use two separate dedicated interfaces.

The interface name of a VLAN logical interface cannot be used for *interface_name*.

The **no** form of this command also clears the failover interface IP address configuration.

Examples

This example shows how to specify the interface and failover VLAN:

```
fwsm(config)# failover lan interface failint vlan 5
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan unit
failover link
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

failover lan unit

To configure the FWSM as the primary FWSM or the secondary FWSM, use the **failover lan unit** command.

failover lan unit {**primary** | **secondary**}

Syntax Description

primary	Specifies the FWSM as the highest failover priority.
secondary	Specifies the FWSM as the lowest failover priority.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The primary and secondary designation for the failover module refers to which module takes over at boot time. This command determines which FWSM becomes active when both modules are booting or when there is contention when both modules are active.

Examples

This example shows how to configure the primary failover unit:

```
fwsm(config)# failover lan unit primary
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover link
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

failover link

To specify the interface name and VLAN for the stateful failover interface, use the **failover link** command. To remove the stateful failover interface, use the **no** form of this command. This link will pass all protocol state information between the active and standby for stateful failover.

[**no**] **failover link** *interface_name* [**vlan** *vlan*]

Syntax Description

interface_name	Name of the FWSM interface that is used for the stateful update information.
vlan *vlan*	(Optional) Sets the VLAN used for stateful update information; see the "Usage Guidelines" section for additional information.

Defaults

Not configured

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **vlan** *vlan* keyword and argument are required when not sharing the failover interface.

The **failover link** command allows you to enable stateful failover. The interface name of a VLAN logical interface cannot be used for *interface_name*. Enter the **no failover link** command to disable the stateful failover feature and also clear the stateful failover interface IP address configuration. If you are not sharing the interface with the failover interface, you must configure the IP address using the **failover interface ip** command and keyword.

Examples

This example shows how to specify the stateful failover interface:

```
fwsm(config)# failover link statefulint vlan 6
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

failover polltime

To specify the failover module and interface monitoring poll frequency, use the **failover polltime** command. To restore the default, use the **no** form of this command.

[**no**] **failover polltime** [**unit**] [**msec**] *time* [**holdtime** *time*]

[**no**] **failover polltime interface** *time*

Syntax Description

unit	(Optional) Sets how often hello messages are sent on the failover link.
msec	(Optional) Specifies that the time interval between messages is in msec.
time	Amount of time between hello messages.
holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the failover link or when the unit begins the testing process for peer failure.
interface *time*	Specifies the poll time for interface monitoring.

Defaults

The defaults are as follows:

- The **unit** poll *time* is 1 second.
- The **interface** *time* is 15 seconds.
- The **holdtime** *time* is 15 seconds.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified.

Usage Guidelines

The **unit** keyword is used for the unit poll time instead of the interface poll time. Set the unit poll time in seconds between 1 and 15. The default is 1 second. If you specify **msec**, you can set the time between 500 and 999 miliseconds.

Set the hold time value in seconds between 3 and 45. The default is the greater of 15 seconds or 3 times the poll time. You cannot enter a value that is less than 3 times the poll time. With a faster poll time, the FWSM can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

For example, if the poll time is 1 second, then a 15-second hold time means that 15 hello messages are missed before the unit is tested for failure.

Note The interval between the stateful information updates is 10 seconds. If you set the poll time greater than 10, then that interval is used.

If a monitored interface does not receive five consecutive hello messages, the FWSM begins the testing process for interface failure.

The interface default is 15 seconds (which means that an interface receives no reply for 75 seconds [5 times the polling interval] before the interface is tested for failure).

When the **unit** or **interface** keywords are not specified, the poll time configured is for the unit (module).

Examples

These examples show how to specify a monitoring poll frequency:

```
fwsm(config)# failover polltime unit 5 holdtime 45
fwsm(config)# failover polltime interface 12
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover replication http
failover reset
monitor-interface
show failover
write standby

failover replication http

To enable HTTP (port 80) connection replication, use the **failover replication http** command. To disable HTTP connection replication, use the **no** form of this command.

[**no**] **failover replication http**

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **failover replicate http** command allows the stateful replication of HTTP sessions in a stateful failover environment. The **no** form of this command disables HTTP replication in a stateful failover configuration. When HTTP replication is enabled, the **show failover** command displays the **failover replicate http** command configuration.

Examples

This example shows how to enable HTTP connection replication:

```
fwsm(config)# failover replication http
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover reset
monitor-interface
show failover
write standby

failover reset

To change the failover modules to an unfailed state after a fault has been corrected, use the **failover reset** command.

failover reset

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **failover reset** command allows you to change the failover modules to an unfailed state after a reset. The **failover reset** command can be entered from either module, but we recommend that you always enter the commands at the active module. Entering the **failover reset** command at the active module will "unfail" the standby module.

Examples

This example shows how to change the failover module to the unfailed state:

```
fwsm(config)# failover reset
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
monitor-interface
show failover
write standby

failover suspend-config-sync

To suspend the failover configuration synchronization, use the **failover suspend-config-sync** command. To reenable the failover configuration synchronization, use the **no** form of this command.

[**no**] **failover suspend-config-sync**

Syntax Description

This command has no arguments or keywords.

Defaults

The **no** form of this command.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command can be run only on an active FWSM.

This command disables interface monitoring and logical updates.

Examples

This example shows how to suspend the failover configuration synchronization:

```
fwsm(config)# failover suspend-config-sync
```

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
monitor-interface
show failover
write standby

filter ftp

To enable File Transfer Protocol (FTP) filtering with a Webserver or Enterprise server, use the **filter ftp** command. To disable FTP filtering, use the **no** form of this command.

[**no**] **filter ftp** *port* [*-port*] | **except** *lcl_ip mask frgn_ip mask* [**allow**] [**interact-block**]

Syntax Description

port [*-port*]	The source and destination port number.
except	Specifes that ports specifed are filtered.
lcl_ip	IP address of the highest security level access point.
mask	Network mask of *source_ip*.
frgn_ip	IP address of the lowest security level access point.
mask	Network mask of *destination_ip*.
allow	(Optional) Allows outbound FTP connections to pass through the FWSM without filtering when the server is unavaliable.
interact-block	(Optional) Prevents users from connecting to the FTP server through an interactive FTP program.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Set the *source_ip* or the *destination_ip* address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

Always specify a specific *destination_mask* value. Use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

Set the *source_mask* to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

Examples

This example shows how to enable FTP filtering:

```
fwsm(config)# filter ftp 21 128.34.65.0 255.255.255.0 140.72.34.0 255.255.255.0 allow
```

or

```
fwsm(config)# filter ftp 21 0 0 0 0 allow
fwsm(config)# filter ftp except 10.192.26.0 255.255.255.0 0.0.0.0 0.0.0.0
```

Related Commands clear filter
show filter

filter https

To enable HTTPS filtering, use the **filter https** command. To disable HTTPS filtering, use the **no** form of this command.

[**no**] **filter https** *port* [*-port*] | **except** *source_ip source_mask destination_ip destination_mask* [**allow**]

Syntax Description

port -port	TCP port range.
except	Creates an exception to a previously specified set of IP addresses (URL only).
source_ip	IP address of the highest security level access point.
source_mask	Network mask of *source_ip*.
destination_ip	IP address of the lowest security level access point.
destination_mask	Network mask of *destination_ip*.
allow	(Optonal) Allows outbound HTTP connections to pass through the FWSM without filtering when the server is unavailable.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Set the *source_ip*, *destination_ip* address, *source_mask,* or *destination_mask* to **0.0.0.0** (or in shortened form, **0**) to specify all hosts. Always specify a specific *destination_mask* value.

Examples

This example shows how to enable HTTP filtering:

```
fwsm(config)# filter https 443 128.35.65.0 255.255.255.0 140.72.34.0 255.255.255.0 allow
```

or

```
fwsm(config)# filter https 443 0 0 0 0 allow
fwsm(config)# filter https except 10.192.26.0 255.255.255.0 0.0.0.0 0.0.0.0
```

Related Commands clear filter
show filter

filter url

To filter HTTP requests from inside users with an external filtering server, use the **filter url** command. To disable HTTP filtering, use the **no** form of this command.

[**no**] **filter url** {*port* [*-port*] | **except**} *lcl_ip mask frgn_ip destination_mask* [**allow**] [**proxy-block**] [**longurl-truncate | longurl-deny**] [**cgi-truncate**]

Syntax Description

http	(Optional) Specifies port 80. You can enter **http** or **www** instead of 80 to specify port 80.
port	Number of the port for inside traffic to use for HTTP.
-port	(Optional) Specifies the port range for inside traffic to use for HTTP.
lcl_ip	IP address of the inside traffic only. Outbound traffic is supported (high to low security level) except if you enable the same security level.
mask	Network mask of *slcl_ip*.
frgn_ip	IP address of the lowest security level access point.
mask	Network mask of *frgn_ip*.
except	Specifies port filtering.
allow	(Optional) Allows outbound connections to pass through the FWSM without filtering when the server is unavailable.
proxy-block	(Optional) Prevents users from connecting to an HTTP proxy server.
longurl-truncate	(Optional) Sends only the originating host name or IP address to the Websense server if the URL is over the URL buffer limit.
longurl-deny	(Optional) Denies the URL request if the URL is over the URL buffer size limit or the URL buffer is not available.
cgi-truncate	(Optional) Truncates CGI URLs to include only the CDI script location and script name (but not parameters).
except	Exempts the specified traffic from filtering.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **http** or **www** keyword can be used to specify port 80/

Set the *lcl_ip* or the *frgn_ip* address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

Always specify a specific*mask* value. Use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

The **filter url** command allows you to prevent outbound users from accessing URLs that you designate using the N2H2 server or Websense server.

Note You must add a filtering server using the **url-server** command before you use any **filter** commands. If you later remove all servers from the configuration, all other **filter** commands are removed.

The **allow** keyword to the **filter** command determines how the FWSM behaves if the N2H2 server or Websense server goes offline. If you use the **allow** keyword with the **filter** command and the N2H2 server or Websense server goes offline, the configured port traffic passes through the FWSM without filtering. Without the **allow** keyword and with the server offline, the FWSM stops the outbound configured port (web) traffic until the server is back online. If another URL server is available, the FWSM passes control to the next URL server.

Note With the **allow** keyword set, the FWSM passes control to an alternate server if the N2H2 server or Websense server goes offline.

Examples

This example shows how to filter all outbound HTTP connections except those from the 10.0.2.54 host:

```
fwsm/context_name(config)# url-server (perimeter) host 10.0.1.1
fwsm/context_name(config)# filter url 80 0 0 0 0
fwsm/context_name(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

This example shows how to block all outbound HTTP connections that are destined to a proxy server that listens on port 8080:

```
fwsm/context_name(config)# filter url 8080 0 0 0 0 proxy-block
```

Related Commands

show filter

firewall

To set the firewall mode to transparent, use the **firewall** command. To set the mode to routed, use the **no** form of this command.

[**no**] **firewall transparent**

Syntax Description

transparent	Specifies transparent firewall mode.

Defaults

Routed firewall mode

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to set the firewall mode to transparent:

```
fwsm(config)# firewall transparent
```

Related Commands

clear firewall
show firewall

fixup protocol

To modify the FWSM protocol fixups to add, delete, or change services and feature defaults, use the **fixup protocol** command. To disable the fixups, use the **no** form of this command.

[**no**] **fixup protocol** *prot* [*option*] *port* [*-port*]

Syntax Description

prot	Protocol fixup to be enabled or disabled: **ftp** [**strict**], **http**, **h323**, **ils**, **mgcp**, **rsh**, **sip**, **skinny**, **smtp**, **sqlnet**, **icmp error**, **dns** [**maximum-length** *length*].
option	(Optional) Option to the inspection function.
port **-***port*	Range of ports to enable the fixup.

Defaults

The defaults are as follows:

- The FWSM fixup protocols and ports are as follows:
  - fixup protocol ftp 21
  - fixup protocol h323 h225 1720
  - fixup protocol h323 ras 1718-1719
  - fixup protocol ils 389
  - fixup protocol rsh 514
  - fixup protocol rtsp 554
  - fixup protocol sip 5060
  - fixup protocol sip udp 5060
  - fixup protocol skinny 2000
  - fixup protocol smtp 25
  - fixup protocol sqlnet 1521
- All **fixup protocol** commands are always present in the configuration and most are enabled.
- **fixup protocol mgcp** is disabled.
- **fixup protocol icmp** is disabled.
- **fixup protocol icmp error** is disabled.
- The FWSM listens to port 21 for FTP.
- **fixup protocol rpc** to port 111 for UDP is enabled.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

fixup protocol ftp

The **fixup protocol ftp** command allows you to specify the listening port or ports for the File Transfer Protocol (FTP). The following describes the features and usage of this command:

- You can use port numbers or supported port literals. See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names.
- The FWSM by default listens to port 21 for FTP.
- You can specify multiple ports.
- You can specify only the port for the FTP control connection and not the data connection. The FWSM stateful inspection dynamically prepares the data connection. For instance, this example is incorrect:

```
fwsm/context_name(config)# fixup protocol ftp 21
fwsm/context_name(config)# fixup protocol ftp 20
```

  This example is correct:

```
fwsm/context_name(config)# fixup protocol ftp 21
```

Caution Use caution when moving FTP to a higher port. For example, if you set the FTP port to 2021 by entering the **fixup protocol ftp 2021** command, all connections that initiate to port 2021 will have their data payload interpreted as FTP commands.

If you disable the FTP fixups with the **no fixup protocol ftp** command, the outbound users can start connections only in passive mode, and all inbound FTP is disabled.

The **strict** keyword to the **fixup protocol ftp** command prevents web browsers from sending embedded commands in FTP requests. Each FTP command must be acknowledged before a new command is allowed. The connections that are sending embedded commands are dropped. The **strict** keyword allows only an FTP server to generate the 227 command and an FTP client to generate the **port** command. The 227 and **port** commands are checked to ensure that they do not appear in an error string.

fixup protocol http

The **fixup protocol http** command allows you to set the port for HTTP traffic application inspection.

Use the **port** keyword to change the default port assignments from 80. Use the *port-port* arguments to apply HTTP application inspection to a range of port numbers.

Note The **no fixup protocol http** command disables the **filter url** command.

HTTP inspection performs these functions:

- URL logging of GET messages
- URL screening through the N2H2 server or Websense servers
- Java and ActiveX filtering

You must configure the URL screening and the Java and ActiveX filtering features with the **filter** command.

fixup protocol icmp

When ICMP fixup is enabled with the **fixup protocol icmp** command, a connection is created for each ICMP traffic stream. An access list is not needed on low security interfaces to allow return traffic (replies) to high security interfaces. You are encouraged to keep the default timeout value for ICMP connections set at the minimum of 2 seconds. This action will help mitigate an attack attempt on the open connection.

fixup protocol icmp error

The **fixup protocol icmp error** command allows you to enable NAT of ICMP error messages. This command creates translations for intermediate hops that are based on the static or network address translation configuration on the FWSM.

The **no fixup protocol icmp error** command allows you to disable the creation of a translation (xlate) for the intermediate nodes that generate ICMP error messages.

fixup protocol dns

Use the **fixup protocol dns** command to specify the maximum Domain Name System (DNS) packet length. DNS requires application inspection so that DNS queries will not be subject to the generic UDP handling based on activity timeouts. Instead, the UDP connections associated with DNS queries and responses are torn down as soon as a reply to a DNS query has been received. This functionality is called DNS Guard.

The port assignment for DNS is not configurable.

Set the maximum length for the DNS fixup as shown in the following example:

```
fwsm(config)# fixup protocol dns maximum-length 1500
fwsm(config)# show fixup protocol dns
fixup protocol dns maximum length 1500
```

Note The FWSM drops DNS packets sent to UDP port 53 that are larger than the configured maximum length. The default value is 512 bytes. A syslog message will be generated when a DNS packet is dropped.

The **no fixup protocol dns** command disables the DNS fixup. The **clear fixup protocol dns** resets the DNS fixup to its default settings (512 byte maximum packet length).

Note If DNS fixup is disabled, the A-record is not sent to NAT and the DNS ID is not matched in requests and responses. By disabling the DNS fixup, the maximum length check on UDP DNS packets can be bypassed and packets greater than the maximum length configured are permitted.

fixup protocol mgcp

Use the **mgcp** command to configure additional support for the MGCP fixup. To use MGCP, you need to configure at least two **fixup protocol** commands as follows:

- One for the port on which the gateway receives commands.
- One for the port on which the call agent receives commands.

A call agent sends commands to the default MGCP port for the gateways, 2427, and a gateway sends commands to the default MGCP port for the call agents, 2727.

This example adds fixup support for the call agents and gateways that use the default ports:

```
fwsm#/context_name(config)# fixup protocol mgcp 2427
fwsm#/context_name(config)# fixup protocol mgcp 2727
```

fixup protocol rpc

The **fixup protocol rpc** command allows you to configure one or more RPC servers and allow a list of services (NFS, NIS, and so on) on those servers for a specified timeout as follows:

- The **active** keyword represents those services for which traffic has already been sent through the FWSM.
- The **no rpc-server active service** *service_type* **server ip_addr** command allows you to remove one of the services from the active list immediately, so that you can block the specified traffic.
- The **clear rpc-server** [**active**] command allows you to clear the entire list of RPC servers or the entire list of active services.

fixup protocol rtsp

The **fixup protocol rtsp** command allows you to configure the FWSM to pass Real Time Streaming Protocol (RTSP) packets. RTSP is used by RealAudio, RealNetworks, Apple QuickTime 4, RealPlayer, and Cisco IP/TV connections.

If you are using Cisco IP/TV, use RTSP TCP port 554 and TCP 8554 as follows:

```
fwsm/context_name(config)# fixup protocol rtsp 554
fwsm/context_name(config)# fixup protocol rtsp 8554
```

These restrictions apply to the **fixup protocol rtsp** command:

- The FWSM will not fix RTSP messages passing through the UDP ports.
- PAT is not supported with the **fixup protocol rtsp** command.
- The FWSM cannot recognize HTTP cloaking where RTSP messages are hidden in the HTTP messages.
- The FWSM cannot perform NAT on the RTSP messages because the embedded IP addresses are contained in the SDP files as part of the HTTP or RTSP messages. The packets could be fragmented, and the FWSM cannot perform NAT on fragmented packets.
- With Cisco IP/TV, the number of NAT processes that the FWSM performs on the SDP part of the message is proportional to the number of program listings in the Content Manager (each program listing can have at least six embedded IP addresses).
- You can configure NAT for the Apple QuickTime 4 or RealPlayer applications. Cisco IP/TV only works with NAT if the Viewer and Content Manager are on the outside network and the server is on the inside network.
- When using RealPlayer, you should properly configure transport mode. For the FWSM, add an **access-list** command from the server to the client or vice versa. For RealPlayer, change the transport mode by clicking **Options>Preferences>Transport>RTSP Settings**.

  If using TCP mode on the RealPlayer application, select the **Use TCP to Connect to Server** and **Attempt to use TCP for all content** check boxes. On the FWSM, you do not need to configure the fixup.

  If using UDP mode on the RealPlayer application, select the **Use TCP to Connect to Server** and **Attempt to use UDP for static content** check boxes. On the FWSM, add the **fixup protocol rtsp** *port* command.

fixup protocol sip

The **fixup protocol sip** command allows you to enable SIP application inspection so that Session Initiation Protocol (SIP) packets are inspected, and then NAT is provided for the appropriate IP addresses.

SIP, as defined by the IETF, enables call handling sessions and two-party audio conferences (calls). SIP works with the Session Description Protocol (SDP) for call signaling. SDP specifies the ports for the media stream. Using SIP, the FWSM can support any SIP Voice over IP (VoIP) gateway or VoIP proxy server. SIP and SDP are defined in the following RFCs:

- SIP: Session Initiation Protocol, RFC 2543
- SDP: Session Description Protocol, RFC 2327

To support SIP, you must inspect calls through the FWSM, signaling messages for the media connection addresses, media ports, and embryonic connections for the media. While the signaling is sent over a well-known destination port (UDP/TCP 5060), the media streams are dynamically allocated because SIP is a text-based protocol that contains IP addresses throughout the text.

FWSM software version 1.1(1) and later versions support PAT for SIP. In FWSM software version 2.2(1) and later versions, you can disable the SIP fixup for both UDP and TCP signaling with the **no fixup protocol sip 5060** command.

Note If you change the value of *port*, SIP will not operate on a different port. You can only turn sip inspection on or off. You cannot change the port.

For additional information about the SIP protocol, refer to RFC 2543. For additional information about the Session Description Protocol (SDP), refer to RFC 2327.

Note Currently, the FWSM does not support NAT TFTP messages.

fixup protocol skinny

The Skinny Client Control Protocol (SCCP or “skinny”) protocol supports IP telephony. An application layer ensures that all SCCP signaling and media packets can traverse the FWSM. The skinny fixup supports both NAT and PAT configurations.

Note The FWSM does not recognize or inspect skinny messages that are fragmented.

Skinny message fragmentation can occur when a call is established that includes a conference bridge. The FWSM tracks the skinny protocol for RTP traffic flow; however, with the skinny messages fragmented, the FWSM cannot correctly RTP.

fixup protocol smtp

The **fixup protocol smtp** command allows you to enable Mail Guard, which lets only mail servers receive the RFC 821, section 4.5.1, commands of HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. All other commands are translated into Xs, which are rejected by the internal server. This situation results in a message such as “500 Command unknown: 'XXX'.” Incomplete commands are discarded.

Note During an interactive SMTP session, various SMTP security rules may reject or deadlock your Telnet session. These rules include the following: SMTP commands must be at least four characters, must be terminated with a carriage return and line feed, and must wait for a response before issuing the next reply.

As of FWSM software version 1.1 and later versions, the **fixup protocol smtp** command allows you to change the characters in the SMTP banner to asterisks except for the "2", "0", and "0" characters. The carriage return and line feed characters are ignored.

In FWSM software version 1.1, all characters in the SMTP banner are converted to asterisks.

fixup protocol sqlnet

The FWSM uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net; however, this value does not agree with IANA port assignments.

Examples

This example shows how to enable the CTIQBE fixup:

```
fwsm/context_name(config)# fixup protocol ctiqbe 2748

fwsm(config)# show fixup protocol ctiqbe
fixup protocol ctiqbe 2748
```

This example shows how to enable access to an inside server running Mail Guard:

```
fwsm/context_name(config)# static (inside,outside) 209.165.201.1 192.168.42.1 netmask
255.255.255.255
fwsm/context_name(config)# access-list acl_out permit tcp host 209.165.201.1 eq smtp any
fwsm/context_name(config)# access-group acl_out in interface outside
fwsm/context_name(config)# fixup protocol smtp 25
```

This example shows how to disable Mail Guard:

```
fwsm/context_name(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask
255.255.255.255
fwsm/context_name(config)# access-list acl_out permit tcp host 209.165.201.1 eq smtp any
fwsm/context_name(config)# access-group acl_out in interface outside
fwsm/context_name(config)# no fixup protocol smtp 25
```

In this example, the **static** command allows you to set up a global address to permit access for outside hosts to the 10.1.1.1 mail server host on the dmz1 interface. (The MX record for DNS needs to point to the 209.165.201.1 address so that mail is sent to this address.) The **access-list** command allows access for any outside users to the global address through the SMTP port (25). The **no fixup protocol** command disables Mail Guard.

This example shows a **fixup protocol ftp** configuration that uses multiple FTP fixups:

```
For an FWSM with two interfaces
:
ip address outside 192.168.1.1 255.255.255.0
ip address inside 10.1.1.1 255.255.255.0
:
: There is an inside host 10.1.1.15 that is
: exported as 192.168.1.15.  This host runs the FTP
: services at port 21 and 1021
:
static (inside, outside) 192.168.1.15 10.1.1.15
:
: Construct an access list to permit inbound FTP traffic to
```

```
: port 21 and 1021
:
access-list outside permit tcp any host 192.168.1.15 eq ftp
access-list outside permit tcp any host 192.168.1.15 eq 1021
access-group outside in interface outside
:
: Specify that traffic to port 21 and 1021 are FTP traffic
:
fixup protocol ftp 21
fixup protocol ftp 1021
```

This example shows how to enable the MGCP fixup on the FWSM:

```
fwsm/context_name(config)# fixup protocol mgcp 2427
fwsm/context_name(config)# fixup protocol mgcp 2727
fwsm(config)# show running-config
: Saved
:
fwsm# Version 2.2(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname fwsm#
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol mgcp 2427
fixup protocol mgcp 2727
fixup protocol sip udp 5060
names
access-list 101 permit tcp any host 10.1.1.3 eq www
access-list 101 permit tcp any host 10.1.1.3 eq smtp
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.23.59.232 255.255.0.0
ip address inside 10.1.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
routing interface inside
route outside 0.0.0.0 0.0.0.0 172.23.59.225 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
```

```
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
dhcprelay server 10.1.1.1 outside
terminal width 80
Cryptochecksum:00000000000000000000000000000000
: end
```

This example shows how to remove the MGCP fixup from the configuration:

```
fwsm/context_name(config)# no fixup protocol mgcp
```

Related Commands

clear fixup
debug
mgcp
show conn
show fixup
timeout

floodguard

To enable or disable the flood defender to protect against flood attacks, use the **floodguard** command.

floodguard {**enable** | **disable**}

Syntax Description

enable	Enables the flood defender.
disable	Disables the flood defender.

Defaults

Enabled

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **floodguard** command allows you to reclaim the FWSM resources if the user authentication (uauth) subsystem runs out of resources. If an inbound or outbound uauth connection is being attacked or overused, the FWSM actively reclaims the TCP user resources.

When the resources deplete, the FWSM lists messages about being out of resources or out of tcpusers.

If the FWSM uauth subsystem is depleted, the TCP user resources in different states are reclaimed. The order depends on the urgency of this situation:

1. Timewait
2. FinWait
3. Embryonic
4. Idle

Examples

This example shows how to enable the **floodguard** command and list the **floodguard** command in the configuration:

```
fwsm/context_name(config)# floodguard enable
fwsm/context_name(config)# show floodguard
```

Related Commands

clear floodguard
show floodguard

format

To format the disk file system, use the **format** command.

format *disk:*

Syntax Description		
	disk:	Device to format.

Defaults

disk: is required.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **format** command allows you to erase all data on the device and then write the file allocation table (FAT) information to the device.

Examples

This example shows how to format the disk system:

```
fwsm(config)# format disk:
format operation may take a while. Continue? [confirm]
```

Related Commands

cd
copy disk
copy flash
copy ftp
copy tftp
dir
mkdir
more
pwd
rename
rmdir
show file

fragment

To provide additional management of packet fragmentation and improve compatibility with the Network File System (NFS), use the **fragment** command.

fragment size *database-limit* [*interface*]

fragment chain *chain-limit* [*interface*]

fragment timeout *seconds* [*interface*]

Syntax Description

size *database-limit*	Sets the maximum number of packets in the fragment database; valid values are from 1 to 30000 or the total number of blocks. See the "Usage Guidelines" section for additional information.
interface	(Optional) FWSM interface. If not specified, the command will apply to all interfaces.
chain *chain-limit*	Specifies the maximum number of packets into which a full IP packet can be fragmented; valid values are from 1 to 8200 packets.
timeout *seconds*	Specifies the maximum number of seconds that a packet fragment will wait to be reassembled after the first fragment is received before being discarded; valid values are from 1 to 30 seconds.

Defaults

The defaults are as follows:

- *chain-limit* is 24.
- *database-limit* is 200.
- *seconds* is 5.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(3)	Support for this command was introduced on the FWSM. This command replaces the **fragguard** command.

Usage Guidelines

By default, the FWSM accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the FWSM to prevent fragmented packets from traversing the FWSM by entering the **fragment chain 1** *interface* command on each interface. Setting the limit to 1 means that all packets must be whole; that is, unfragmented.

If a large percentage of the network traffic through the FWSM is NFS, additional tuning may be necessary to avoid database overflow. See system log message 209003 for additional information.

In an environment where the MTU between the NFS server and client is small, such as a WAN interface, the **chain** keyword may require additional tuning. In this case, we recommend using NFS over TCP to improve efficiency.

If you do not specify the *interface*, the command applies to all interfaces.

Setting the *database-limit* of the **size** keyword to a large value can make the FWSM more vulnerable to a Denial of Service (DoS) attack by fragment flooding. Do not set the *database-limit* equal to or greater than the total number of blocks in the 1550 or 16384 pool. See the **show block** command for more details. The default values will limit DoS due to fragment flooding to that interface only.

Examples

This example shows how to prevent fragmented packets on the outside and inside interfaces:

```
fwsm/context_name(config)# fragment chain 1 outside
fwsm/context_name(config)# fragment chain 1 inside
```

Continue entering the **fragment chain 1** *interface* command for each additional interface on which you want to prevent fragmented packets.

This example shows how to configure the outside fragment database to limit a maximum size of 2000, a maximum chain length of 45, and a wait time of 10 seconds:

```
fwsm(config)# fragment size 2000 outside
fwsm(config)# fragment chain 45 outside FWSM(config)# fragment timeout 10 outside
fwsm(config)#
```

Related Commands

clear fragment

ftp mode

To set the FTP mode, use the **ftp mode** command. To disable the FTP mode, use the **no** form of this command.

[**no**] **ftp mode passive**

Syntax Description

passive	Sets the FTP mode to passive.

Defaults

passive

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to set the FTP mode to passive:

```
fwsm(config)# ftp mode passive
```

Related Commands

clear ftp
show ftp

global

To create entries from a pool of global addresses, use the **global** command. To remove access to a *nat_id*, a Port Address Translation (PAT) address, or an address range within a *nat_id,* use the **no** form of this command.

[**no**] **global** [ext_*interface_name*] *nat_id* {*global_ip* [-*global_ip*] [**netmask** *global_mask*]} | **interface**

Syntax Description

ext_interface_name	(Optional) Name of the external network where you use these global addresses.
nat_id	Positive number that is shared with the **nat** command that groups the **nat** and **global** commands together; valid ID numbers can be any positive number up to 2147483647.
global_ip	Global IP addresses that the FWSM shares among its connections.
-global_ip	(Optional) Secondary global IP address.
netmask *global_mask*	(Optional) Specifies the network mask for the *global_ip*.
interface	Specifies the IP address of the external network overloaded for PAT.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **global** command allows you to define a pool of global addresses. The global addresses in the pool provide an IP address for each outbound connection and for those inbound connections that result from outbound connections. Make sure that the associated **nat** and **global** commands have the same *nat_id*.

Note The number of address translations allowed is per each FWSM. The FWSM supports 2,048 address translations for the **nat** command, 1,051 address translations for the **global** command, and 2,048 address translations for the **static** command. The FWSM also supports up to 4,096 access control entries (ACEs) in ACLs used for policy NAT.

The **global** command cannot use names with a "-" (dash) character, because the "-" character is interpreted as a range specifier instead of as part of the object name.

This command syntax is used for PAT only:

global [*interface_name*] *nat_id* {*global_ip*} [**netmask** *global_mask*] | **interface**}

After changing or removing a **global** command, use the **clear xlate** command.

The *global_ip* argument is one or more global IP addresses that the FWSM shares among its connections. If the external network is connected to the Internet, you must register each global IP address with the Network Information Center (NIC).

You can specify a range of IP addresses by separating the addresses with a dash (-).

You can create a PAT **global** command by specifying a single IP address. You can have one PAT **global** command per interface. A PAT can support up to 65,535 xlate objects.

When specifying the *global_mask,* if subnetting is in effect, use the subnet mask; for example, use 255.255.255.128. If you specify an address range that overlaps subnets, **global** will not use the broadcast or network addresses in the pool of global addresses. For example, if you use **255.255.255.224** and an address range of **209.165.201.1-209.165.201.30**, the 209.165.201.31 broadcast address and the 209.165.201.0 network address are not included in the pool of global addresses.

Examples

This example shows how to declare two global pool ranges and a PAT address. The **nat** command permits all inside users to start connections to the outside network:

```
fwsm/context_name(config)# global (outside) 1 209.165.201.1-209.165.201.10 netmask
255.255.255.224
fwsm/context_name(config)# global (outside) 1 209.165.201.12 netmask 255.255.255.224
Global 209.165.201.12 will be Port Address Translated
fwsm/context_name(config)# nat (inside) 1 0 0
fwsm/context_name(config)# clear xlate
```

This example shows how to create a global pool from two contiguous pieces of a Class C address and give the perimeter hosts access to this pool of addresses to start connections on the outside interface:

```
fwsm/context_name(config)# global (outside) 1000 209.165.201.1-209.165.201.14 netmask
255.255.255.240
fwsm/context_name(config)# global (outside) 1000 209.165.201.17-209.165.201.30 netmask
255.255.255.240
fwsm/context_name(config)# nat (perimeter) 1000 0 0
```

Related Commands

clear global
show global

help

To display help information for the command specified, use the **help** command.

help *command*

?

Syntax Description

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

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged, Privileged and Configuration

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **help** or **?** command allows you to display help information about all commands. You can see help for an individual command by entering the command name followed by a "**?**" (question mark).

If you do not specify a command name, all commands that are available in the current privilege level and mode are displayed.

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

This example shows how you can display help information by following the command name with a question mark:

```
FWSM(config)# enable ?
Usage: enable password [<pw>] [level <level>] [encrypted]
        no enable password level <level>
        show enable
FWSM(config)# enable
```

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

```
FWSM(config)# ?

At the end of show <command>, use the pipe character '|' followed by:
begin|include|exclude|grep [-v] <regular_exp>, to filter show output.

aaa             Enable, disable, or view TACACS+, RADIUS or LOCAL
                user authentication, authorization and accounting ...
```

hostname

To change the host name in the FWSM command line prompt, use the **hostname** command.

hostname *newname*

Syntax Description

newname	New host name for the FWSM and is displayed in the FWSM prompt; this name can have up to 63 alphanumeric characters.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **hostname** command allows you to change the host name label on prompts. The default host name is FWSM.

Note Changing the host name causes the fully qualified domain name to change. Once the fully qualified domain name is changed, delete the RSA key pairs with the **ca zeroize rsa** command and delete the related certificates with the **no ca identity** *ca_nickname* command.

Examples

This example shows how to change a host name:

```
fwsm(config)# hostname spinner
spinner(config)# hostname fwsm
fwsm(config)#
```

Related Commands

clear hostname
show hostname

http

To enable the FWSM HTTP server and specify the clients that are permitted to access it, use the **http** command. To disable the feature, use the **no** form of this command.

[**no**] **http** *ip_address* [*netmask*] [*interface_name*]

[**no**] **http server enable**

Syntax Description

ip_address	Host or network authorized to initiate an HTTP connection to the FWSM.
netmask	(Optional) Network mask for the **http** *ip_address*.
interface_name	(Optional) FWSM interface name on which the host or network initiating the HTTP connection resides.
server enable	Enables the HTTP server required to run PDM.

Defaults

If you do not specify a netmask, the default is 255.255.255.255 regardless of the class of IP address.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For access, the FWSM Device Manager requires that the FWSM have an enabled HTTP server.

Access from any host is allowed if you specify 0.0.0.0 0.0.0.0 (or 0 0) for *ip_address* and *netmask*.

Examples

This example shows how to enable the HTTP server and specify one host:

```
fwsm/context_name(config)# http 16.152.1.11 255.255.255.255 outside
```

This example shows how to enable the HTTP server and specify any host:

```
fwsm/context_name(config)# http 0.0.0.0 0.0.0.0 inside
```

Related Commands

clear http
show http

icmp

To configure access rules for Internet Control Message Protocol (ICMP) traffic that terminates at an interface, use the **icmp** command. To remove access rules, use the **no** form of this command.

[**no**] **icmp** {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *interface_name*

Syntax Description

permit	Permits access if the conditions are matched.
deny	Denies access if the conditions are matched.
ip_address	IP address of the host sending ICMP messages to the interface.
net_mask	Mask to be applied to *ip_address*.
icmp_type	(Optional) ICMP message type as described in Table 2-9.
interface_name	Interface name.

Defaults

All inbound traffic through any interface is denied.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

By default, the FWSM denies all inbound traffic through all interfaces. Based on your network security policy, you should consider configuring the FWSM to deny all ICMP traffic at the outside interface, or any other interface by using the **icmp** command.

The **icmp** command controls the ICMP traffic that is received by the FWSM. If no ICMP control list is configured, then the FWSM accepts all ICMP traffic that terminates at any interface (including the outside interface), except that the FWSM does not respond to ICMP echo requests that are directed to a broadcast address.

The **icmp deny** command disables pinging to an interface, and the **icmp permit** command allows you to enable pinging to an interface. With pinging disabled, the FWSM cannot be detected on the network.

For traffic that is routed through the FWSM only, you can use the **access-list** or **access-group** commands to control the ICMP traffic that is routed through the FWSM.

We recommend that you grant permission for the ICMP unreachable message type (type 3). Denying ICMP unreachable messages disables ICMP path maximum transmission unit (MTU) discovery, which can halt IPSec and Point-to-Point Tunneling Protocol (PPTP) traffic. See RFC 1195 and RFC 1435 for more information.

If an ICMP control list is configured, then the FWSM uses a first match to the ICMP traffic followed by an implicit deny all. That is, if the first matched entry is a permit entry, the ICMP packet continues to be processed. If the first matched entry is a deny entry or an entry is not matched, the FWSM discards the ICMP packet and generates the %FWSM-3-313001 syslog message. An exception is when an ICMP control list is not configured; in that case, a permit is assumed.

The syslog message is as follows:

%FWSM-3-313001: Denied ICMP type=*type*, code=*code* from *source_address* on interface *interface_number*

If this message appears, you should contact the peer's system administrator.

Table 2-9 lists the possible ICMP type values.

Table 2-9 ICMP Type Literals

ICMP Type	Literal
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

Examples

This example shows how to deny all ICMP traffic, including ping requests, to the outside interface:

```
fwsm/context_name(config)# icmp deny any outside
```

Continue entering the **icmp deny any** *interface* command for each additional interface on which you want to deny ICMP traffic.

This example shows how to deny all ping requests and permit all unreachable messages at the outside interface:

```
fwsm/context_name(config)# icmp deny any echo-reply outside
fwsm/context_name(config)# icmp permit any unreachable outside
```

This example shows how to permit the echo-reply from host 172.16.2.15 inbound only. This means that the echo inbound from host 172.16.2.15 is denied. The FWSM can ping the host, but the host cannot ping the FWSM.

```
fwsm/context_name(config)# icmp permit host 172.16.2.15 echo-reply outside
```

Related Commands

clear icmp
show icmp

ignore lsa mospf (router ospf submode)

To stop the FWSM from sending syslog messages when the router receives a link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets, use the **ignore lsa mospf** subcommand. To restore the sending of these syslog messages, use the **no** form of this command.

[**no**] **ignore lsa mospf**

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show router ospf** command displays the configured **router ospf** subcommands.

Type 6 Multicast OSPF (MOSPF) packets are unsupported.

Examples

This example shows how to suppress syslog messaging:

```
fwsm(config)# router ospf 1
fwsm(config-router)# ignore lsa mospf
```

Related Commands

router ospf
show ignore lsa mospf
show router ospf

interface

To create an interface and enter the interface submode to configure OSPF parameters and shut down an interface, use the **interface** command.

interface *interface_name*

Syntax Description

interface_name	Interface name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was changed.

Usage Guidelines

When you are in the single context mode and routed firewall mode and enter the interface submode, the following commands are available:

- **ospf**—Allows you to configure specific OSPF parameters. See the **ospf (interface submode)** command.
- **exit/quit**—Exits from the submode.
- [**no**] **shutdown**—Sets the interface so that no traffic is sent or accepted.

When you are in the multiple context mode and transparent firewall mode and you enter the interface submode, the **shutdown** command is available:

- **shutdown**—Stops traffic from flowing through an interface. In the system context or single mode, the **shutdown** command stops traffic from flowing through all interfaces attached to a specified VLAN. In the user context, the **shutdown** command stops traffic from flowing through that one interface.

Examples

This example shows how to enter the interface submode:

```
fwsm(config)# interface inside
fwsm(config-interface) shutdown
```

Related Commands

clear interface stats
ip address
nameif
ospf (interface submode)
show interface
shutdown

ip address

To identify addresses for network interfaces, use the **ip address** command.

Command used in transparent mode:

ip address *ip_address* [*mask*] [**standby** *sby_ip_addr*]

Command used in routed mode:

ip address *interface_name ip_address* [*mask*] [**standby** *sby_ip_addr*]

Syntax Description

ip_address	FWSM module's network interface IP address.
mask	(Optional) Network mask of *ip_address*.
standby	(Optional) Specifies the secondary or failover peer module.
sby_ip_addr	(Optional) IP address for the failover module.
interface_name	Interface name designated by the **nameif** command.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Note To remove the standby interface IP address, set the *sby_ip_addr* to zero. To remove the IP address, set the IP address to zero and the mask to 255.255.255.255.

The **ip address** command allows you to assign an IP address to each interface. Use the **show ip** command to see which addresses are assigned to the network interfaces. If you make a mistake while entering this command, reenter the command with the correct information. The **clear ip** command clears all interface IP addresses. The **clear ip** command does not affect the **ip verify reverse-route** commands.

Note The **clear ip** command stops all traffic through the FWSM.

After changing the **ip address** command, use the **clear xlate** command.

Always specify a network mask with the **ip address** command. If you let the FWSM assign a network mask based on the IP address, you may not be permitted to enter subsequent IP addresses if another interface's address is in the same range as the first address. For example, if you specify an inside interface address of 10.1.1.1 without specifying a network mask and then try to specify 10.1.2.2 for a perimeter interface mask, the FWSM displays the error message, "Sorry, not allowed to enter IP address on same network as interface *n*." To fix this problem, reenter the first command specifying the correct network mask.

Do not set the netmask to all 255s, such as 255.255.255.255. This action stops access on the interface. Instead, use a network address of 255.255.255.0 for Class C addresses, 255.255.0.0 for Class B addresses, or 255.0.0.0 for Class A addresses.

The FWSM configurations using failover require a separate IP address for each network interface on the standby module. The system IP address is the address of the active module. When the **show ip** command is executed on the active module, the current IP address is the same as the system IP address. When the **show ip** command is executed on the standby module, the current IP address is the failover IP address that is configured for the standby module.

Examples

This example shows how to set the IP address in transparent mode:

```
fwsm/context_name(config)# ip address 209.165.201.2 255.255.255.224
```

This example shows how to display IP addresses in routed mode:

```
fwsm/context_name(config)# show ip address
System IP Addresses:
        ip address inside 36.7.1.1 255.255.0.0
        ip address shared 22.7.24.1 255.255.0.0
        ip address dmz 38.7.1.1 255.255.0.0
        ip address mgmt 10.7.24.1 255.255.0.0
        ip address outside 37.7.1.1 255.255.0.0
Current IP Addresses:
        ip address inside 36.7.1.1 255.255.0.0
        ip address shared 22.7.24.1 255.255.0.0
        ip address dmz 38.7.1.1 255.255.0.0
        ip address mgmt 10.7.24.1 255.255.0.0
        ip address outside 37.7.1.1 255.255.0.0
```

Related Commands

clear ip address
clear ip verify reverse-path
nameif
show ip address
show ip verify

ip local pool

To define a local address pool, use the **ip local pool** command.

ip local pool *poolname ip1* [*-ip2*]

Syntax Description

poolname	FWSM module's network interface IP address.
ip1	IP address of the first local address pool.
-ip2	(Optional) IP address of a local pool.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The DHCPD address pools and the IP local pool cannot overlap.

Examples

This example shows how to define a local address pool:

```
fwsm/context_name(config)# ip local pool 209.165.201.2 255.255.255.224
```

Related Commands

clear ip address
dhcpd
show ip address
show ip verify
telnet
who

ip prefix-list

To configure an IP prefix list, use the **ip prefix-list** command.

[**no**] **ip prefix-list** *list-name* [**seq** *seq-value*] {**permit** | **deny**} *prefix/len* [**ge** *min-value*] [**le** *max-value*]

Syntax Description

list-name	Specifies the IP prefix list name.
seq *seq-value*	(Optional) Specifies the sequence value; valid values are from 1 to 2147483646.
permit	(Optional) Permits the prefix list.
deny	Denies the prefix list.
prefix/len	Specifies the prefix list and prefix list length.
ge *min-value*	(Optional) Minimum length value.
le *max-value*	(Optional) Maximum length value.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to configure an IP prefix list:

```
fwsm/context_name(config)# ip prefix-list soccer seq 23 permit 10.0.0.0/8
```

Related Commands

clear ip address
dhcpd
show ip address
show ip verify
telnet
who

ip verify reverse-path

To enable both ingress and egress filtering to verify addressing and route integrity, use the **ip verify reverse-path** command. To disable **ip verify reverse-path** filtering for an individual interface from the configuration, use the **no** form of this command.

[**no**] **ip verify reverse-path interface** *int_name*

Syntax Description

interface *int_name*	Name of an interface that you want to protect from a Denial-of-Service (DoS) attack.

Defaults

Disabled

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **ip verify reverse-path** command allows you to do a route lookup based on the source address. This feature is called reverse path forwarding because the route lookup is typically based on the destination address, not the source address. With this command enabled, packets are dropped if there is no route found for the packet or the route found does not match the interface on which the packet arrived.

The **ip verify reverse-path** command allows you to specify which interfaces to protect from an IP spoofing attack using network ingress and egress filtering, which is described in RFC 2267. This command is disabled by default and provides Unicast Reverse Path Forwarding (Unicast RPF) functionality for the FWSM.

Because of the danger of IP spoofing in the IP protocol, you need to take measures to reduce this risk when possible. Unicast RPF, or reverse route lookup, prevents such manipulation under certain circumstances.

Note The **ip verify reverse-path** command depends on the existence of a default route entry in the configuration for the outside interface that has 0.0.0.0 0.0.0.0 in the **route** command for the IP address and network mask.

The **ip verify reverse-path** command provides both ingress and egress filtering. Ingress filtering checks inbound packets for IP source address integrity and is limited to addresses for networks in the enforcing entity's local routing table. If the incoming packet does not have a source address that is represented by a route, then it is impossible to know whether the packet has arrived on the best return path to its originator.

Egress filtering verifies that the packets that are destined for hosts outside the managed domain have IP source addresses verifiable by routes in the enforcing entity's local routing table. If an exiting packet does not arrive on the best return path to the originator, then the packet is dropped and the activity is logged. Egress filtering prevents internal users from launching attacks using IP source addresses outside of the local domain because most attacks use IP spoofing to hide the identity of the attacking host. Egress filtering makes tracing the origin of an attack much easier. When employed, egress filtering enforces which IP source addresses are obtained from a valid pool of network addresses. Addresses are kept local to the enforcing entity and are easily traceable.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.
- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Noninitial packets are checked to ensure that they arrived on the same interface used by the initial packet.

Note Before using this command, add the static **route** commands for every network that can be accessed on the interfaces that you wish to protect. Enable this command only if routing is fully specified. If you do not specify routing, the FWSM stops traffic on the interface that you specify.

Use the **show interface** command to view the number of dropped packets, which appears in the "unicast rpf drops" counter.

Examples

This example shows how to protect traffic between the inside and outside interfaces and provide **route** commands for two networks, 10.1.2.0 and 10.1.3.0, that connect to the inside interface through a hub:

```
fwsm/context_name(config)# ip address inside 10.1.1.1 255.255.0.0
fwsm/context_name(config)# route inside 10.1.2.0 255.255.0.0 10.1.1.1 1
fwsm/context_name(config)# route inside 10.1.3.0 255.255.0.0 10.1.1.1 1
fwsm/context_name(config)# ip verify reverse-path interface outside
fwsm/context_name(config)# ip verify reverse-path interface inside
```

The **ip verify reverse-path interface outside** command protects the outside interface from network ingress attacks from the Internet. The **ip verify reverse-path interface inside** command protects the inside interface from network egress attacks from users on the internal network.

Related Commands

clear ip address
dhcpd
show ip address
show ip verify

isakmp

To configure the Internet Security Association Key Management Protocol (ISAKMP) for IPSec Internet Key Exchange (IKE), use the **isakmp** commands. To disable IKE, use the **no** form of this command.

[**no**] **isakmp client configuration address-pool local** *pool-name* [*interface-name*]

[**no**] **isakmp enable** *interface-name*

[**no**] **isakmp identity** {**address | hostname**}

[**no**] **isakmp keepalive** *seconds* [*retry_seconds*]

[**no**] **isakmp key** *keystring* **address** *peer-address* [**netmask** *mask*] [**no-xauth**] [**no-config-mode**]

[**no**] **isakmp peer fqdn | ip** *fqdn | ip* [**no-xauth**] [**no-config-mode**]

Syntax Description

client configuration address-pool	Configures the client pool and the client address pool.
local *pool-name*	Specifies the name of a local address pool to allocate the dynamic client IP.
interface-name	(Optional) Name of the interface on which to enable ISAKMP negotiation.
enable *interface-name*	Enables the specified interface.
identity address	Specifies the IP address of the host exchanging ISAKMP identity information.
identity hostname	Specifies the name of the tunnel peer as configured using the **name** command.
keepalive *seconds*	Specifies the keepalive interval; valid values are from 10 and 3600 seconds.
retry_seconds	(Optional) Time interval before a keepalive message is sent if a keepalive response is not received from the previous request; valid values are from 2 to 60 seconds.
key *keystring*	Specifies the authentication preshared key.
address *peer-address*	Specifies the IPSec peer's IP address for the preshared key.
netmask *mask*	(Optional) Netmask of 0.0.0.0. can be entered as a wildcard indicating that the key could be used for any peer that does not have a key associated with its specific IP address.
no-xauth	(Optional) Associates a given preshared key with a gateway and allows an exception to the Xauth feature that is enabled by the **crypto map client authentication** command.
no-config-mode	(Optional) Associates a given preshared key with a gateway and allows an exception to the IKE mode configuration feature that is enabled by the **crypto map client configuration address** command.
peer fqdn *fqdn*	Fully qualified domain name of the security gateway peer.

Defaults

The defaults are as follows:

- The local pool interface is **outside**.
- The ISAKMP identity is **isakmp identity hostname**.
- *retry_seconds* is **2** seconds.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **no** forms of the **isakmp** command are as follows:

- The **no isakmp client configuration address-pool local** command restores the default value.
- The **no isakmp enable** command disables IKE.
- The **no isakmp identity** command resets the ISAKMP identity to the default value of the host name.
- The **no isakmp key address** command deletes a preshared authentication key and its associated IPSec peer address.
- The **no isakmp peer fqdn** *fqdn* **no-xauth | no-config-mode** command disables the **isakmp peer fqdn** *fqdn* **no-xauth | no-config-mode** command that you previously enabled.

isakmp client configuration address-pool local

The **isakmp client configuration address-pool local** command is used to configure the IP address local pool to reference IKE.

The **isakmp enable** command is used to enable the ISAKMP negotiation on the interface on which the IPSec peer communicates with the FWSM. ISAKMP is not enabled by default.

isakmp identity

The **isakmp** command allows you to define the ISAKMP identity that the FWSM uses when participating in the IKE protocol.

When two peers use IKE to establish IPSec security associations, each peer sends its ISAKMP identity to the remote peer. It sends either its IP address or host name depending on how each has its ISAKMP identity set. By default, the FWSM's ISAKMP identity is set to the host name. Set the FWSM and its peer's identities in the same way to avoid an IKE negotiation failure using the **name** command. A failure could be due to either the FWSM or its peer not recognizing its peer's identity.

Note If you use RSA signatures as your authentication method in your IKE policies, we recommend that you set each participating peer's identity to the host name. Otherwise, the ISAKMP security association to be established during phase 1 of IKE may fail.

The sections that follow describe each **isakmp** command.

isakmp keepalive

The **isakmp keepalive** *seconds* [*retry_seconds*] command allows you to set the keepalive lifetime interval. The keepalive interval can be between 10 and 3600 seconds. The retry interval can be between 2 and 60 seconds, with the default as 2 seconds. The retry interval is the interval between retries after a keepalive response has not been received. You can specify the keepalive lifetime interval without specifying the retry interval, but you cannot specify the retry interval without specifying the keepalive lifetime interval.

isakmp key address

To configure a preshared authentication key and associate the key with an IPSec peer address or host name, use the **isakmp key address** command.

You would configure the preshared key at both peers whenever you specify the preshared key in an IKE policy. Otherwise, you cannot use the policy because it is not submitted for matching by the IKE process.

You can enter a netmask of 0.0.0.0 as a wildcard. This wildcard (or netmask) indicates that any IPSec peer with a given valid preshared key is a valid peer.

Note The FWSM or any IPSec peer can use the same authentication key with multiple peers, but using a unique authentication key between each pair of peers is a much more secure process.

Configure a preshared key that is associated with a given security gateway to be distinct from a wildcard, preshared key (preshared key plus a netmask of 0.0.0.0) that is used to identify and authenticate the remote VPN clients.

Use the **no-xauth** or **no-config-mode** keywords only if the following criteria are met:

- You are using the preshared key authentication method within your IKE policy.
- The security gateway and VPN client peers terminate on the same interface.
- Xauth or IKE mode configuration is enabled for VPN client peers.

The **isakmp key** *keystring* **address** *ip-address* [**no-xauth**] [**no-config-mode**] command allows you to configure a preshared authentication key, associate the key with a given security gateway's address, and make an exception to the enabled Xauth, IKE mode configuration features, or both (the most common case) for this peer.

Both Xauth and IKE mode configurations are designed for remote VPN clients. Xauth allows the FWSM to challenge the peer for a username and password during IKE negotiation. IKE mode configuration enables the FWSM to download an IP address to the peer for dynamic IP address assignment. Most security gateways do not support Xauth and IKE mode configuration.

You cannot enable Xauth or IKE mode configuration on an interface when terminating a Layer 2 Tunneling Protocol (L2TP) IPSec tunnel using the Microsoft L2TP/IPSec client v1.0 (which is available on Windows NT, Windows XP, Windows 98, and Windows ME OS). Instead, you can do either of the following:

- Use a Windows 2000 L2TP/IPSec client.
- Use the **isakmp key** *keystring* **address** *ip-address* **netmask** *mask* **no-xauth no-config-mode** command to exempt the L2TP client from Xauth and IKE mode configuration. However, if you exempt the L2TP client from Xauth or IKE mode configuration, you must group all the L2TP clients with the same ISAKMP preshared key or certificate and have the same fully qualified domain name.

If you have the **no-xauth** keyword configured, the FWSM does not challenge the peer for a username and password. Similarly, if you have the **no-config-mode** keyword configured, the FWSM does not attempt to download an IP address to the peer for dynamic IP address assignment.

Use the **no key** *keystring* **address** *ip-address* [**no-xauth**] [**no-config-mode**] command to disable the **key** *keystring* **address** *ip-address* [**no-xauth**] [**no-config-mode**] command that you previously enabled.

isakmp peer fqdn no-xauth | no-config-mode

Use the **isakmp peer fqdn** *fqdn* **no-xauth | no-config-mode** command only if the following criteria are met:

- You are using the RSA signatures authentication method within your IKE policy.
- The security gateway and VPN client peers terminate on the same interface.
- Xauth or IKE mode configuration is enabled for VPN client peers.

The **isakmp peer fqdn** *fqdn* **no-xauth | no-config-mode** command allows you to identify a peer that is a security gateway and make an exception to the enabled Xauth, IKE mode configuration, or both (the most common case) features for this peer.

Both Xauth and IKE mode configuration are designed for remote VPN clients. Xauth allows the FWSM to challenge the peer for a username and password during IKE negotiation. The IKE mode configuration enables the FWSM to download an IP address to the peer for dynamic IP address assignment. Most security gateways do not support Xauth and IKE mode configurations.

If you have the **no-xauth** keyword configured, the FWSM does not challenge the peer for a username and password. If you have the **no-config-mode** keyword configured, the FWSM does not attempt to download an IP address to the peer for dynamic IP address assignment.

Note If you use RSA signatures as your authentication method in your IKE policies, we recommend that you set each participating peer's identity to the host name using the **isakmp identity hostname** command. Otherwise, the ISAKMP security association to be established during phase 1 of IKE may fail.

Examples

This example shows how to reference IP address local pools to IKE with "mypool" as the pool-name:

```
fwsm/context_name(config)# isakmp client configuration address-pool local mypool outside
```

This example shows how to disable IKE on the inside interface:

```
fwsm/context_name(config)# no isakmp enable inside
```

This example shows how to use preshared keys between the two FWSMs (FWSM 1 and FWSM 2) that are peers, and set both their ISAKMP identities to the host name.

At the FWSM 1, the ISAKMP identity is set to the host name:

```
fwsm/context_name(config)# isakmp identity hostname
```

At the FWSM 2, the ISAKMP identity is set to the host name:

```
fwsm/context_name(config)# isakmp identity hostname
```

This example shows how to set the "sharedkeystring" as the authentication key to share between the FWSM and its peer that is specified by an IP address of 10.1.0.0:

```
fwsm/context_name(config)# isakmp key sharedkeystring address 10.1.0.0
```

This example shows how to use a wildcard, preshared key. The “sharedkeystring” is the authentication key to share between the FWSM and its peer (in this case, a VPN client) that is specified by an IP address of 0.0.0.0. and a netmask of 0.0.0.0.

```
fwsm/context_name(config)# isakmp key sharedkeystring address 0.0.0.0 netmask 0.0.0.0
```

This example shows how to use the **no-xauth** and **no-config-mode** keywords with three FWSM peers that are security gateways. These security gateways terminate IPSec on the same interface as the VPN clients. Both Xauth and IKE mode configurations are enabled requiring that an exception be made to these two features for each security gateway. The example shows each security gateway peer with a unique preshared key to share with the FWSM. The peers’ IP addresses are 10.1.1.1, 10.1.1.2, and 10.1.1.3; the netmask of 255.255.255.255 is specified.

```
fwsm/context_name(config)# isakmp key secretkey1234 address 10.1.1.1 netmask
255.255.255.255 no-xauth no-config-mode
fwsm/context_name(config)# isakmp key secretkey4567 address 10.1.1.2 netmask
255.255.255.255 no-xauth no-config-mode
fwsm/context_name(config)# isakmp key secretkey7890 address 10.1.1.3 netmask
255.255.255.255 no-xauth no-config-mode
```

This example shows how to use the **no-xauth** and **no-config-mode** keywords with three FWSM peers that are security gateways. These security gateways terminate IPSec on the same interface as the VPN clients. Both the Xauth and IKE mode configuration features are enabled requiring that an exception be made to these two features for each security gateway. Each security gateway peer’s fully qualified domain name is specified.

```
fwsm/context_name(config)# isakmp peer fqdn hostname1.example.com no-xauth no-config-mode
fwsm/context_name(config)# isakmp peer fqdn hostname2.example.com no-xauth no-config-mode
fwsm/context_name(config)# isakmp peer fqdn hostname3.example.com no-xauth no-config-mode
```

Related Commands

ca authenticate
crypto dynamic-map
crypto ipsec security-association lifetime
crypto map client
isakmp policy
show isakmp policy

isakmp policy

To configure specific Internet Key Exchange (IKE) algorithms and parameters within the IPSec Internet Security Association Key Management Protocol (ISAKMP) framework for the Authentication Header (AH) and Encapsulating Security Payload (ESP) IPSec protocols, use the **isakmp policy** command. To return to the default settings, use the **no** form of this command.

[**no**] **isakmp policy** *priority* **authentication** {*pre-share* | *rsa-sig*}

[**no**] **isakmp policy** *priority* **encryption** {**des** | **3des**}

[**no**] **isakmp policy** *priority* **group** {**1** | **2**}

[**no**] **isakmp policy** *priority* **hash** {**md5** | **sha**}

[**no**] **isakmp policy** *priority* **lifetime** *seconds*

Syntax Description

priority	Priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
authentication *pre-share*	Specifies the preshared keys that are the authentication method.
authentication *rsa-sig*	Specifies the RSA signatures that are the authentication method.
encryption des	Specifies that the 56-bit DES-CBC is the encryption algorithm that is used in the IKE policy.
encryption 3des	Specifies that the Triple DES encryption algorithm is used in the IKE policy.
group 1	Specifies that the 768-bit Diffie-Hellman group is used in the IKE policy.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 is used in the IKE policy.
hash md5	Specifies that MD5 (HMAC variant) is the hash algorithm used in the IKE policy.
hash sha	Specifies that SHA-1 (HMAC variant) is the hash algorithm used in the IKE policy.
lifetime *seconds*	Specifies the number of seconds that each security association should exist before expiring; valid values are from 120 to 86,400 seconds (one day).

Defaults

The defaults are as follows:

- The ISKMP policy encryption is **des**.
- The Diffie-Hellman group is **group 1**.
- The hash algorithm is **sha** (HMAC variant).
- The **lifetime** *seconds* is **86400** seconds (one day).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **isakmp policy** command allows you to negotiate IPSec security associations and enable IPSec secure communications.

isakmp policy authentication

The **isakmp policy authentication** command allows you to specify the authentication method within an IKE policy. IKE policies define a set of parameters to be used during IKE negotiation.

If you specify RSA signatures, you must configure the FWSM and its peer to obtain certificates from a CA. If you specify preshared keys, you must separately configure these preshared keys within the FWSM and its peer.

isakmp policy encryption

The **isakmp policy-encryption** command allows you to specify the encryption algorithm that is used within an IKE policy. DES (**des**) and 3DES (**3des**) are the supported encryption algorithms. (IKE policies define the set of parameters to be used during IKE negotiation.)

isakmp policy group

The **isakmp policy group** command allows you to specify the Diffie-Hellman group that is used in an IKE policy. IKE policies define a set of parameters that are used during IKE negotiation.

There are two group options: 768-bit (DH Group 1) and the 1024-bit (DH Group 2). The 1024-bit Diffie-Hellman Group provides stronger security but requires more CPU time to execute.

Use the **no isakmp policy group** command to reset the Diffie-Hellman group identifier to the default value of group 1 (768-bit Diffie Hellman).

Note Cisco VPN Client version 3.x uses Diffie-Hellman group 2, and Cisco VPN Client 3000 version 2.5/2.6 uses Diffie-Hellman group 1.

isakmp policy hash

The **isakmp policy hash** command allows you to specify the hash algorithm that is used in an IKE policy. IKE policies define a set of parameters that are used during IKE negotiation.

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

To reset the hash algorithm to the default value of SHA-1, use the **no isakmp policy hash** command.

isakmp policy lifetime

The **isakmp policy lifetime** command allows you to specify the lifetime of an IKE security association before it expires and reset the security association lifetime to the default value of 86,400 seconds (one day).

When IKE begins negotiations, it looks to agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by a security association at each peer. The security association is retained by each peer until the security association's lifetime expires. Before a security association expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec security associations. New security associations are negotiated before current security associations expire.

To save setup time for IPSec, configure a longer IKE security association lifetime. However, the shorter the lifetime, the more secure the IKE negotiation is likely to be.

Note When the FWSM initiates an IKE negotiation between itself and an IPSec peer, an IKE policy can be selected only if the lifetime of the peer's policy is shorter than or equal to the lifetime of its policy. If the lifetimes are not equal, the shorter lifetime is selected.

Examples

This example shows how to set an isakmp policy:

```
fwsm/context_name(config)# isakmp policy 93 group 2
```

This example shows how to use the **isakmp policy authentication** command to set the authentication method of RSA signatures used within the IKE policy with the priority number of 40:

```
fwsm/context_name(config)# isakmp policy 40 authentication rsa-sig
```

This example shows how to set the 3DES algorithm used within the IKE policy with the priority number of 40:

```
fwsm/context_name(config)# isakmp policy 40 encryption 3des
```

This example shows how to use the **isakmp policy group** command to set group 2, the 1024-bit Diffie Hellman, used within the IKE policy with the priority number of 40:

```
fwsm/context_name(config)# isakmp policy 40 group 2
```

This example shows how to use the **isakmp policy hash** command to set the MD5 hash algorithm used within the IKE policy with the priority number of 40:

```
fwsm/context_name(config)# isakmp policy 40 hash md5
```

This example shows how to use the **isakmp policy lifetime** command to set the lifetime of the IKE security association to 50,400 seconds (14 hours) within the IKE policy with the priority number of 40:

```
fwsm/context_name(config)# isakmp policy 40 lifetime 50400
```

Related Commands

ca authenticate
crypto dynamic-map
crypto ipsec security-association lifetime
crypto map client
isakmp
show isakmp

kill

To terminate a Telnet session, use the **kill** command.

kill *telnet_id*

Syntax Description

telnet_id	Telnet session ID as displayed by the **who** command.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **kill** command allows you to terminate a Telnet session. Use the **who** command to see the Telnet session ID value. When you kill a Telnet session, the FWSM lets any active commands terminate and then drops the connection without warning the user.

Note You cannot terminate the Ethernet Out-of-Band Channel (EOBC) Telnet session from the switch to the system using the **kill** command.

Examples

This example shows the output from the **show who** command, which is used to list the active Telnet sessions, and the use of the **kill** command to end Telnet session 2:

```
fwsm/context_name(config)# show who
2: From 10.10.54.0
fwsm/context_name(config)# kill 2
```

Related Commands

telnet
who

limit-resource (class submode)

To set the resource limitations for all members of the class, use the **limit-resource** command after you enter the **class** command and enter the class subconfiguration mode. To turn off resource limiting, use the **no** form of this command.

[**no**] **limit-resource** {[**rate**] *resource_name* | **all**} *number* [**%**]

Syntax Description

rate	(Optional) Sets the limit for qualifying individual resources to be *number* per second.
resource_name	Name of the resource that you want to limit.
all	Sets the limits for many resources, including resources that cannot be set individually.
number	Number that is greater than or equal to 0.
number **%**	(Optional) Percentage of resource limitations when used with the *number* argument; see the "Usage Guidelines" section for additional information.

Defaults

Conns [rate] unlimited
Fixups [rate] unlimited
Syslogs [rate] unlimited
Conns unlimited
Hosts unlimited
IPSec 5
Mac-addresses 65535
PDM 5
SSH 5
Telnet 5
Xlates unlimited

Command Modes

Security Context Mode: Multiple

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Enter the **limit-resource** command multiple times until you set all the limits required.

You can set the rate limited resource types:

- connections 1000000 concurrent 100000 per second
- fixups

- syslogs 30000 per second

You can also set the absolute limit types:

- Conns Connections
- Hosts Hosts
- IPSec IPSec Mgmt Tunnels
- Mac-addresses MAC Address table entries
- PDM PDM Connections
- SSH SSH Sessions
- Telnet Telnet Sessions
- Xlates XLATE Objects

When you enter an *individual resource_name*, the limit overrides the limit set for all.

Use the **all** keyword with *number %*, not an absolute value. The general resources that cannot be set individually include the following:

- SMTP fixups
- AAA UXLATE
- AAA Uauthor
- Established connections
- PIFs
- Fixup packets per second
- ARP entries
- All chunks
- Memory (heap)
- TCP proxies
- TCP selects
- TCP users
- UDP users
- Logger blocks
- Answers

For the *number %* keyword and argument, you can enter the following:

- 0—This value sets the resource to unlimited.
- An absolute value (integer)—Do not use with the **all** keyword. See the total number of resources available in the *resource_name* description. You can assign more than the total number across all classes if you want to oversubscribe the device.
- A percentage (real number)—Follow the number by the percent sign (**%**). For example, 0.001%. You can assign more than 100% across all classes if you want to oversubscribe the device.

  Table 2-10 lists the resource types and the limits. See also the **show resource types** command.

Table 2-10 Resource Names and Limits

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
mac-addresses	N/A	65 K concurrent	For transparent firewall mode, the number of MAC addresses allowed in the MAC address table.
conns	N/A	999,900 concurrent 102,400 per second (rate)	TCP or UDP connections between any two hosts, including connections between one host and multiple other hosts. **Note** For concurrent connections, the FWSM allocates half of the limit to each of two network processors (NPs) that accept connections. Typically, the connections are divided evenly between the NPs. However, in some circumstances, the connections are not evenly divided, and you might reach the maximum connection limit on one NP before reaching the maximum on the other. In this case, the maximum connections allowed is less than the limit you set. The NP distribution is controlled by the switch based on an algorithm. You can adjust this algorithm on the switch, or you can adjust the connection limit upward to account for the inequity.
fixups	N/A	10,000 per second (rate)	Application inspection.
hosts	N/A	256 K concurrent	Hosts that can connect through the FWSM.
ipsec	1 minimum 5 maximum concurrent	10 concurrent	IPSec sessions
pdm	1 minimum 5 maximum concurrent	32 concurrent	FDM management sessions. **Note** FDM sessions use two HTTPS connections: one for monitoring that is always present, and one for making configuration changes that is present only when you make changes. For example, the system limit of 32 FDM sessions represents a limit of 64 HTTPS sessions.
ssh	1 minimum 5 maximum concurrent	100 concurrent	SSH sessions.

Table 2-10 Resource Names and Limits (continued)

Resource Name	Minimum and Maximum Number per Context	Total Number for System	Description
syslogs	N/A	30,000 per second (rate)	System messages. **Note** The FWSM can support 30,000 messages per second for messages sent to the FWSM terminal or buffer. If you send messages to a syslog server, the FWSM supports 25,000 per second.
telnet	1 minimum 5 maximum concurrent	100 concurrent	Telnet sessions.
xlates	N/A	256 K concurrent	NAT translations.

When you create a class, you do not set aside a portion of the resources for each context that is assigned to the class; instead, you set the maximum limit for a context. If you oversubscribe the resources, or allow some resources to be unlimited, you can use up some of the resources that are assigned to another context.

You can set the limit for all resources together (a general limit), or you can set the limit for resources individually. However, only some resources can be limited individually while many more resources are covered by a general limit. If you include both types of limits (individual and general), the FWSM uses the limits for individual resources (if present) and applies the general limit to all other resources.

You can oversubscribe the FWSM by assigning more than 100 percent of the resources across all contexts. For example, you can set the Bronze class to limit all resources to 1 percent per context, and then assign 150 contexts to the class. Make sure that the contexts do not all reach their limits at the same time.

The FWSM allows you to assign unlimited access to one or more resources in a class instead of a percentage or absolute number. When a resource is unlimited, the contexts can use as much of the resource as the system has available. Setting unlimited access is similar to oversubscribing the FWSM, except that you have less control over how much you oversubscribe the system.

Examples

This example shows how to set the resource limitations to limit fixups to 100 per second under a class named gold:

```
fwsm(config-class)# class gold
fwsm(config-class)# limit-resource rate fixup 100
```

Related Commands

clear resource usage
show resource allocation
show resource types
show resource usage

log

To generate syslog message 106100 for an ACE, use the **log** keyword in the **access-list** commands.

log [**disable**] | [*level*] | [**default**] | [**interval** *secs*]]

Syntax Description

disable	(Optional) Disables syslog messaging. See the "Usage Guidelines" section for additional information.
level	(Optional) Syslog level; valid values are from 0 to 7. See the "Usage Guidelines" section for additional information.
default	(Optional) Specifies that a syslog message 106100 is generated for an ACE. See the "Usage Guidelines" section for additional information.
interval *secs*	(Optional) Specifies the time interval at which to generate a 106100 syslog message; valid values are from 1 to 600 seconds.

Defaults

The default ACL logging behavior (the **log** keyword is not specified) is that if a packet is denied, then message 106023 is generated. If a packet is permitted, then no syslog message is generated.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

When you specify the **log** optional keyword, it generates syslog message 106100 for the ACE to which it is applied. (syslog message 106100 is generated for every matching permit or deny ACE flow passing through the FWSM.) The first-match flow is cached. Subsequent matches increment the hit count displayed in the **show access-list** command for the ACE, and new 106100 messages are generated at the end of the interval that is defined by **interval** *secs* if the hit count for the flow is not zero.

The default ACL logging behavior (the **log** keyword is not specified) is that if a packet is denied, then message 106023 is generated. If a packet is permitted, then no syslog message is generated.

You can specify an optional syslog *level* (0–7) for the generated syslog messages (106100). If no *level* is specified, the default level is 6 (informational) for a new ACE. If the ACE already exists, then its existing log level remains unchanged.

If you specify the **log disable** optional keyword, the access list logging is completely disabled. No syslog message, including message 106023, is generated.

The **log default** optional keyword restores the default access list logging.

Note Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for additional information about logging.

Examples

This example shows what happens when you enable an access-list **log** optional keyword:

```
fwsm/context_name(config)# access-list outside-acl permit ip host 1.1.1.1 any log 7
interval 600
fwsm/context_name(config)# access-list outside-acl permit ip host 2.2.2.2 any
fwsm/context_name(config)# access-list outside-acl deny ip any any log 2
fwsm/context_name(config)# access-group outside-acl in interface outside
```

The previous example shows the use of access-list logging in an ICMP context:

1. An ICMP echo request (1.1.1.1 -> 192.168.1.1) arrives on the outside interface.
2. An ACL called **outside-acl** is applied for the access check.
3. The packet is permitted by the first ACE of **outside-acl** that has the **log** optional keyword enabled.
4. The log flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) has not been cached, so the following syslog message is generated and the log flow is cached:

   ```
   106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
   inside/192.168.1.1(8) hit-cnt 1 (first hit)
   ```

5. Twenty packets arrive on the outside interface within the next 10 minutes (600 seconds). Because the log flow has been cached, the log flow is located and the hit count of the log flow is incremented for each packet.
6. At the end of 10 minutes, this syslog message is generated and the hit count of the log flow is reset to 0:

   ```
   106100: access-list outside-acl permitted icmp outside/1.1.1.1(0) ->
   inside/192.168.1.1(8) hit-cnt 20 (300-second interval)
   ```

7. No packets arrive on the outside interface within the next 10 minutes, so the hit count of the log flow remains 0.
8. At the end of 20 minutes, the cached flow (ICMP, 1.1.1.1, 0, 192.168.1.1, 8) is deleted because of the 0 hit count.

To disable a **log** optional keyword without removing the ACE, enter the **access-list** *id* **log disable** command.

When removing an ACE with a **log** optional keyword enabled using the **no access-list** command, you do not need to specify all the **log** options. The ACE is removed if its permit or deny rule is used to uniquely identify it. However, removing an ACE (with a **log** optional keyword enabled) does not remove the associated cached flows. You must remove the entire ACL to remove the cached flows. When a cached flow is flushed due to the removal of an ACL, a syslog message is generated if the hit count of the flow is nonzero.

Use the **clear access-list** command to remove all the cached flows.

Related Commands

access-list alert-interval
clear access-list

log-adj-changes (router ospf submode)

To configure the router to send a syslog message when an Open Shortest Path First (OSPF) neighbor goes up or down, use the **log-adj-changes** subcommand. To turn off this function, use the **no** form of this command.

log-adj-changes [**detail**]

no log-adj-changes

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Defaults

Enabled

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show router ospf** command allows you to display the configured **router ospf** subcommands.

The **show ip ospf** displays other details for the OSFP processes running.

The **log-adj-changes** subcommand is enabled by default.

Examples

This example shows how to enable system log messages:

```
fwsm(config)# router ospf 1
fwsm(config-router)# log-adj-changes detail
fwam(config-router)#
```

Related Commands

router ospf
show log-adj-changes
show ip ospf
show router ospf

logging

To enable syslog and SNMP logging, use the **logging** command. To disable syslog and SNMP logging, use the **no** form of this command.

[**no**] **logging** {**on** | **buffered** *level* | **console** *level* | **facility** *facility* | **history** *level* | {**message** *syslog_id* [**level** *level*]} | **monitor** *level* | **queue** *queue_size* | **standby** | **timestamp** | **trap** *level*}

[**no**] **logging device-id** {**hostname** | **ipaddress** *interface_name* | **string** *text* | **context-name**}

[**no**] **logging host** *in_intf syslog_ip* [*port/port*] [**format emblem**] [**interface** *if1* [*if2*] ...]

[no] logging buffer-size *bytes*

Syntax Description

on	Sends syslog messages to all output locations.
buffered *level*	Sends the specified syslog level messages to an internal buffer that can be viewed with the **show logging** command; see the "Usage Guidelines" section for valid values.
console *level*	Specifies that the specified syslog level messages appear on the FWSM console as each message occurs; see the "Usage Guidelines" section for valid values.
facility *facility*	Specifies the syslog facility; valid values are **16** (LOCAL0) through **23** (LOCAL7).
history *level*	Specifies the SNMP message level for sending syslog traps; see the "Usage Guidelines" section for valid values.
message *syslog_id*	Specifies a message number to disallow or allow.
level *level*	(Optional) Specifies the syslog message level as a number or string; see the "Usage Guidelines" section for valid values.
monitor *level*	Specifies that the syslog messages appear on Telnet sessions to the FWSM console; see the "Usage Guidelines" section for valid values.
queue *queue_size*	Specifies the size of the queue for storing syslog messages. The *queue_size* length limit of the log queue is 0, unlimited..
standby	Allows the failover standby module to send syslog messages.
timestamp	Specifies that syslog messages that are sent to the syslog server should have a time-stamp value on each message.
trap *level*	Specifies the logging level for syslog messages only.
device-id	Specifies that the device ID of the FWSM is included in the syslog message.
hostname	Specifies to use the host name of the FWSM to uniquely identify the syslog messages from the FWSM.
ipaddress *interface_name*	Specifies to use the IP address of the specified FWSM interface to uniquely identify the syslog messages from the FWSM.
string *text*	Specifies the text string to uniquely identify the syslog messages from the FWSM.
context-name	Specifies the context.
host	Specifies a syslog server that will receive the messages that are sent from the FWSM.
in_intf	Interface on which the syslog server resides.

syslog_ip	Syslog server's IP address.
port	(Optional) Port from which the FWSM sends either UDP or TCP syslog messages; valid values are as follows: • The UDP port is from 1025 to 65535. • The TCP port is from 1025 to 65535.
format emblem	(Optional) Enables EMBLEM format logging for each syslog server.
interface	(Optional) Specifies that only the messages that are associated with those interfaces listed are sent to the host.
if1 [*if2*] ...]	Specifies the interface.
buffer-size *bytes*	Specifies the buffer size in bytes. Range is from 4096, to 32768 bytes.

Defaults

The defaults are as follows:

- EMBLEM format logging is disabled.
- The *facility* is 20 (LOCAL4).
- The *queue_size* is 512 messages.
- The *port* is as follows:
  - UDP port is 514
  - TCP port is 1470
- The **logging device-id** command is disabled.
- The **logging console** command is disabled.
- The **logging standby** command is disabled.
- The logging buffer-size minimum is 4096 bytes.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode for the command, configuration mode for the **no** form of this command.

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **logging** command allows you to enable or disable sending informational messages to the console, to a syslog server, or to an SNMP management station. You can stop all logging with the **no logging on** command.

The FWSM provides more information in messages that are sent to a syslog server than at the console, but the console provides enough information to permit effective troubleshooting.

Caution Do not use the **logging console** command because it degrades system performance. Instead, use the **logging buffered** command to start logging, the **show logging** command to see the messages, and the **clear logging** command to clear the buffer to make viewing the most current messages easier.

The **aaa accounting** **authentication enable console** command causes syslog messages to be sent (at syslog level 4) each time that the configuration is changed from the serial console.

logging console

You can limit the types of messages that appear on the console with *level*. We recommend that you do not use this command because its use degrades FWSM performance.

logging facility

Hosts file the messages that are based on the *facility* number in the message.

logging device-id

The **logging device-id** command allows you to display a unique device ID in non-EMBLEM format syslog messages that are sent to the syslog server.

If enabled, the FWSM displays the device ID in all non-EMBLEM-formatted syslog messages. However, it does not affect the syslog message text that is in EMBLEM format.

Note The device ID part of the syslog message is viewed through the syslog server only and not directly on the FWSM.

If you use the **ipaddress** keyword, the device ID becomes the specified FWSM interface IP address, regardless of the interface from which the message is sent. This keyword provides a single consistent device ID for all messages that are sent from the device.

The maximum length **string** *text* is 32 characters with no white space (blanks) allowed.

logging history

The **logging history** command allows you to set the SNMP message level for sending syslog traps..

logging host

The **logging host** *ip_address* **format emblem** command allows you to enable EMBLEM-format logging for each syslog server. EMBLEM-format logging is available for UDP syslog messages only (because the resource management environment (RME) syslog analyzer supports only UDP syslog messages). If you enable EMBLEM-format logging for a particular syslog host, then the messages are sent to that host. If you also enable the **logging timestamp** keyword, the messages with a time stamp are sent.

You can use multiple **logging host** commands to specify additional servers that would all receive the syslog messages. However, a server can only be specified to receive either UDP or TCP, not both. The FWSM sends only TCP syslog messages to the FWSM Syslog Server (PFSS).

You can display only the *port* and *protocol* values that you previously entered by using the **write terminal** command and finding the command in the listing—the TCP protocol is listed as 6 and the UDP protocol is listed as 17. TCP ports work only with the FWSM syslog server. The *port* must be the same port at which the syslog server listens.

logging level

The *level* that you specify indicates that you want that *level* and those less than the *level*. For example, if that *level* is 3, the syslog displays 0, 1, 2, and 3 messages**.** Possible number and string *level* values are as follows:

- **0—emergencies**—System unusable messages
- **1—alerts**—Take immediate action
- **2—critical**—Critical condition
- **3—errors**—Error message
- **4—warnings**—Warning message
- **5—notifications**—Normal but significant condition
- **6—informational**—Information message
- **7—debugging**—Debug messages and log FTP commands and WWW URLs

logging message

The **logging message** *syslog_id* **level** *level* command allows you to change the level of syslog messages. The **no logging message** command cannot block the "%FWSM-6-199002: FWSM startup completed. Beginning operation" syslog message.

If a message is listed in syslog as %FWSM-1-101001, use "101001" as the *syslog_id*. Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Firewall Services Module System Message Guide* for more information about message numbers.

logging queue

The **logging queue** command allows you to specify the size of the syslog message queue for the messages that are waiting to be processed. When traffic is heavy, the messages may be discarded.

Set the queue size before the syslog messages are processed. 0 (zero) indicates unlimited (subject to available block memory), and the minimum is one message.

logging standby

The **logging standby** command allows you to enable the failover standby module to send syslog messages. Using this command ensures that the standby module's syslog messages stay synchronized if failover occurs. However, this feature causes twice as much traffic on the syslog server.

logging timestamp

The **logging timestamp** command allows you to require that the clock is set.

logging trap

The **logging trap** command allows you to set the syslog message level.

Troubleshooting

If you are using TCP as the logging transport protocol, the FWSM stops passing traffic as a security measure if the FWSM is unable to reach the syslog server, the syslog server is misconfigured (such as with PFSS, for example), or the disk is full. (UDP-based logging does not prevent the FWSM from passing traffic if the syslog server fails.)

Examples

This example shows how to start logging to the internal buffer which can be viewed with the **show logging** command:

```
fwsm/context_name(config)# logging buffered debugging
```

This example shows how to specify the host name of the FWSM in syslog messages:

```
fwsm(config)# logging device-id hostname
fwsm(config)# show logging Syslog logging: enabled
    Facility: 20
    Timestamp logging: enabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: hostname "FWSM"
    Logging Buffer size: 4096 bytes
fwsm(config)# "
```

This example shows how to display the output of the **logging queue** and **show logging queue** commands:

```
fwsm(config)# logging queue 0
fwsm(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

In this example, the **logging queue** command is set to 0, which means that you want an unlimited number of messages. All syslog messages are to be processed. The **show logging queue** command shows that 5 messages are queued, 3513 messages was the largest number of messages in the queue at one time since the FWSM was last booted, and that 1 message was discarded. Even though the queue was set for unlimited, the messages are discarded if the amount of block memory is exhausted.

This example shows how to display the **show logging** command output when the TCP syslog server is unreachable. The FWSM stops passing traffic, and logging to the inside is set as **disabled**:

```
fwsm/context_name(config)# show logging
Syslog logging: enabled
    Timestamp logging: enabled
    Standby logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 827 messages logged
    Trap logging: level debugging, facility 20, 840 messages logged
   Logging to inside 10.1.1.1 tcp/1468 disabled
```

This example shows how to change the level of a syslog message and display its current and default level:

```
fwsm/context_name(config)# logging message 403503
fwsm/context_name(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

fwsm/context_name(config)# logging message 403503 level 1
fwsm/context_name(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

fwsm/context_name(config)# logging message 403503 level 6
fwsm/context_name(config)# show logging message 403503
```

```
syslog 403503: default-level errors, current-level informational (enabled)

fwsm/context_name(config)# logging message 403503 level 3
fwsm/context_name(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

Related Commands

clear logging rate-limit
show logging
show logging rate-limit

logging rate-limit

To limit the rate at which the syslog is generated, use the **logging rate-limit** command. To disable rate limiting, use the **no** form of this command.

[**no**] **logging rate-limit** {**unlimited** | {*num* [*interval*]}} **message** *syslog_id*

[**no**] **logging rate-limit** {**unlimited** | *num* [*interval*]} **level** *syslog_level*

Syntax Description

unlimited	Disables rate limiting.
num	Number at which the syslog is to be rate limited.
interval	(Optional) Time interval (in seconds) over which the syslogs should be limited.
message	Suppresses reporting of this syslog message.
syslog_id	ID of the syslog to suppress reporting.
level *syslog_level*	Sets the level above which the FWSM suppresses messages to the syslog host.

Defaults

interval is **1**.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The syslog message suppression levels are as follows:

- 0—System Unusable
- 1—Take Immediate Action
- 2—Critical Condition
- 3—Error Message
- 4—Warning Message
- 5—Normal but significant condition
- 6—Informational
- 7—Debug Message

Examples

This example shows how to limit the rate of syslog generation:

```
fwsm(config)# logging rate-limit 5 message 106023
fwsm(config)# logging rate-limit 10 60 level 7
```

Related Commands

clear logging rate-limit
show logging
show logging rate-limit

login

To initiate the login prompt on the FWSM for starting a session or access another privilege level or command mode as a specific user, use the **login** command.

login

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **login** command allows you to log into the FWSM, another privilege level, or command mode using the local user authentication database that is created with the **username** command. This command is available in unprivileged mode.

After you log in, you can use the **logout**, **exit**, or **quit** commands to go back to unprivileged mode.

Examples

This example shows how to initiate the login prompt:

```
fwsm> login
Username:
```

Related Commands

logout
privilege
username

logout

To exit from the current user profile and return to the unprivileged mode, use the **logout** command.

logout

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **logout** command allows you to log out of the FWSM, another privilege level, or command mode using the local user authentication database that is created with the **username** command. This command is available in unprivileged mode.

You can use the **logout**, **exit**, or **quit** commands to go back to unprivileged mode.

Examples

This example shows how to log out:

```
fwsm> logout
fwsm>
```

Related Commands

login
privilege
username

mac-address-table static

To add a list of interfaces and associated MAC addresses to the Layer 2 forwarding table, use the **mac-address-table static** command. To delete the list, use the **no** form of this command.

[**no**] **mac-address-table static** *interface_name mac*

Syntax Description

interface_name	Interface name.
mac	Source MAC address in *aabbcc.ddeeff.gghhii* form.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: transparent mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **mac-address-table static** command allows you to enter static MAC addresses into the Layer 2 forwarding table. You can enter the **mac-address-table static** command multiple times with the same *interface_name* argument to group a set of MAC addresses.

The **clear mac-address-table** *interface_name* command allows you to remove only the interface entries learned dynamically from the Layer 2 forwarding table. The command does not remove the entries configurred by the **mac-addres-table static** command. To remove the MA C address table static entries, use the **no mac-address-table static c**ommand.

The **show mac-address-table static** command allows you to display only the static MAC entries on the Layer 2 forwarding table.

Examples

This example shows how to configure a list of interfaces and MAC addresses:

```
fwsm/context_name(config)# mac-address-table static inside 5678.aeb0.4325
Added <5678.aeb0.4325> to the bridge table

fwsm(config)# show mac-address static
interface                  mac  address          type      Age(min)
-------------------------------------------------------------------
inside                    0000.0bff.0000          static
```

Related Commands

clear mac-address-table
mac-address-table aging-time
show mac-address-table

mac-address-table aging-time

To specify the aging time for the bridge timeout value in the Layer 2 forwarding table, use the **mac-address-table aging-time** command. To remove the bridge timeout value from the configuration, use the **no** form of this command.

[**no**] **mac-address-table aging-time** *minutes*

Syntax Description

minutes	Specifies the bridge timeout aging time period in minutes, the range is from 5 to 720 minutes.

Defaults

The timeout is 5 minutes.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: transparent mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To remove the bridge timeout aging time value use the no form of this command to return to the default value.

Examples

This example shows how to configure the bridge timeout aging time:

```
fwsm/context_name(config)# mac-address-table aging-time 5
```

Related Commands

clear mac-address-table
mac-address-table static
show mac-address-table

mac-learn

To control the learning of MAC addresses per interface, use the **mac-learn** command. To delete the list, use the **no** form of this command.

[**no**] **mac-learn** *interface_name* **disable**

Syntax Description

interface_name	Interface name.
disable	Disables MAC learning on the specified interface.

Defaults

Enabled

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: transparent mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear mac-learn** command allows you to disable the MAC address learning from all of the interfaces.

The **show mac-learn** command allows you to display the status of the MAC address learning feature on all of the interfaces.

Examples

This example shows how to disable MAC address learning on an interface, display the results, and then clear the MAC learning on all interfaces:

```
FWSM(config)# mac-learn inside disable
Disabling learning on inside
FWSM(config)# show mac-learn
interface                          mac learn
-----------------------------------------
 inside                              disabled
 outside                             enabled
FWSM(config)# clear mac-learn
Enabling learning on inside
Enabling learning on outside
FWSM(config)#
```

Related Commands

clear mac-learn
show mac-learn

match (route map submode)

To define the conditions for redistributing routes from one routing protocol into another, use the **match** command in the route-map submode. To restore the default settings, use the **no** form of this command.

[**no**] **match** [**interface** *interface_name* | **metric** *metric_value* | **ip address** *acl_id* | **route-type** {**local** | **internal** | [**external** [**type-1** | **type-2**]]} | **nssa-external** [**type-1** | **type-2**] | **ip next-hop** *acl_id* | **ip route-source** *acl_id*]

Syntax Description

interface *interface_name*	(Optional) Name of the interface.
metric *metric_value*	(Optional) Metric value; valid values are from 0 to 2147483647.
ip-address *acl_id*	(Optional) Specifies routes that have a destination network tha matches a standard ACL.
route-type local	(Optional) Specifies routes that are local to a specified autonomous system.
route-type internal	(Optional) Specifies routes that are internal to a specified autonomous system.
route-type external	(Optional) Specifies routes that are external to a specified autonomous system.
type-1 | type-2	(Optional) Specifies the type of Open Shortest Path First (OSPF) metric routes that are external to a specified autonomous system.
nssa-external	(Optional) OSPF metric type for routes that are external to a not-so-stubby area (NSSA).
ip next-hop *acl_id*	(Optional) Specifies routes that have a next-hop router address that matches a standard ACL.
ip route-source *acl_id*	Specifies routes that have been advertised by routers that match a standard ACL.

Defaults

The default is **type-2**.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

All keywords are optional but when using the **match** command, only one keyword is required.

The **match ip next-hop** and **match ip route-source** commands can accept more than one *acl_id*; they accept *acl_id* [...*acl_id*].

Examples

This example shows how to define the redistributed routes:

```
fwsm(config-route-map)# match interface inside
fwsm(config-route-map)# match ip next-hop 10
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip next-hop (route map submode)
match ip route-source (route map submode)
match metric (route map submode)
route-map
set metric (route map submode)
set metric-type (route map submode)

match interface (route map submode)

To distribute any routes that have their next hop out one of the interfaces specified, use the **match interface** command in the route-map submode. To remove the match interface entry, use the **no** form of this command.

[**no**] **match interface** {*interface-name1 interface-name2...*}

Syntax Description

interface-name	Name of the interface. More than one interface can be specified.

Defaults

No match interfaces are defined.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the interface-type interface-number arguments.

The **route-map global configuration** command and the **match** and **set route-map** configuration commands allow you to 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—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is 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 give the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions that are given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

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. If you want to modify only some data, you must configure a second route map section and specify an explicit match.

Examples

This example shows that the routes with their next hop out Ethernet interface 0 is distributed:

```
fwsm(config)# route-map name
fwsm(config-route-map)# match interface inside
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip next-hop (route map submode)
match ip route-source (route map submode)
match metric (route map submode)
route-map
set metric (route map submode)
set metric-type (route map submode)

match ip next-hop (route map submode)

To redistribute any routes that have a next-hop router address that is passed by one of the access lists specified, use the **match ip next-hop** command in the route-map submode. To remove the next-hop entry, use the **no** form of this command.

[**no**] **match ip next-hop** {*acl-id...*}

Syntax Description

acl-id	Number of a standard access lists; valid values are from 1 to 199.

Defaults

Routes are distributed freely, without being required to match a next-hop address.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-number or access-list-name argument.

The **route-map global** configuration command and the **match** and **set route-map** configuration commands allow you to define the conditions for redistributing routes from one routing protocol into another. Each **route-map** command has a **match** and **set** commands that are associated with it. The **match** commands specify the match criteria—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is 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 give the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

When you are passing 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 and specify an explicit match.

Examples

This example shows how to distribute routes that have a next-hop router address passed by access list 5 or 80:

```
fwsm(config)# route-map name
fwsm(config-route-map)# match ip next-hop 5 80

fwsm(config)# route-map name
fwsm(config-route-map)# match ip next-hop 5
fwsm(config-route-map)# match ip next-hop 80
fwsm(config-route-map)#
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip route-source (route map submode)
match metric (route map submode)
route-map
set metric (route map submode)
set metric-type (route map submode)

match ip route-source (route map submode)

To redistribute routes that have been advertised by routers and access servers at the address that is specified by the access lists, use the **match ip route-source** command in the route-map submode. To remove the route-source entry, use the **no** form of this command.

[**no**] **match ip route-source** {*acl-id ...*}

Syntax Description

acl-id	Number of a standard access lists; valid values are from 1 to 199.

Defaults

No filtering on a route source.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

An ellipsis (...) in the command syntax indicates that your command input can include multiple values for the access-list-number or access-list-name argument.

The **route-map global** configuration command and the **match** and **set route-map** configuration commands allow you to 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—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular 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 give the **match** commands in any order. All **match** commands must "pass" to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

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 and specify an explicit match. The next-hop and source-router address of the route are not the same in some situations.

Examples

This example shows how to distribute routes that have been advertised by routers and access servers at the addresses specified by access lists 5 and 80:

```
fwsm(config)# route-map name
fwsm(config-route-map)# match ip route-source 5 80

fwsm(config)# route-map name
fwsm(config-route-map)# match ip route-source 5
fwsm(config-route-map)# match ip route-source 80
fwsm(config-route-map)#
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip next-hop (route map submode)
match metric (route map submode)
route-map
set metric (route map submode)
set metric-type (route map submode)

match metric (route map submode)

To redistribute routes with the metric specified, use the **match metric** command in the route-map submode. To remove the entry, use the **no** form of this command.

[**no**] **match metric** *number*

Syntax Description

number	Route metric, which can be an IGRP five-part metric; valid values are from 0 to 4294967295.

Defaults

No filtering on a metric value.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set route-map** configuration commands allow you to 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—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is 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. The **match** commands can be given 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** forms of the **match** commands remove the specified match criteria.

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 and specify an explicit match.

Examples

This example shows how to redistrube routes with the metric 5:

```
fwsm(config)# route-map name
fwsm(config-route-map)# match metric 5
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip next-hop (route map submode)
match ip route-source (route map submode)
route-map
set metric (route map submode)
set metric-type (route map submode)

match route-type (route map submode)

To redistribute routes of the specified type, use the **match route-type** command in the route-map submode. To remove the route type entry, use the **no** form of this command.

[**no**] **match route-type** {**local** | **internal** | {**external** [**type-1** | **type-2**]} | **nssa-external** | [**type-1** | **type-2**]}

Syntax Description

local	Specifies the locally generated Border Gateway Protocol (BGP) routes.
internal	Specifies the Open Shortest Path First (OSPF) intra-area and interarea routes or Enhanced Interior Gateway Routing Protocol (EIGRP) internal routes.
external	Specifies the OSPF external routes or EIGRP external routes.
type-1	(Optional) Specifies the route type 1.
type-2	(Optional) Specifies the route type 2.
nssa-external	Specifies the external not-so-stubby-area (NSSA).

Defaults

This command is disabled by default.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **route-map global** configuration command and the **match** and **set route-map** configuration commands allow you to 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—the conditions under which redistribution is allowed for the current **route-map** command. The **set** commands specify the set actions—the particular redistribution actions to perform if the criteria that is 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 give the **match** commands in any order. All **match** commands must “pass” to cause the route to be redistributed according to the set actions given with the **set** commands. The **no** forms of the **match** commands remove the specified match criteria.

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 and specify an explicit match.

For OSPF, the **external type-1** keywords match only type 1 external routes and the **external type-2** keywords match only type 2 external routes.

Examples

This example shows how to redistribute internal routes:

```
fwsm(config)# route-map name
fwsm(config-route-map)# match route-type internal
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip next-hop (route map submode)
match metric (route map submode)
route-map
set metric (route map submode)
set metric-type (route map submode)

member (context submode)

To determine the class to which a context belongs, use the **member** command in the context submode. To remove a context from a class, use the **no** form of this command.

member *class_name*

[**no**] **member** *class_name*

Syntax Description

class_name	Class name.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The class sets resource limitations for each class member. To use the settings of a class, assign the context to the class. All contexts belong to the default class if they are not assigned to another class; you do not have to actively assign a context to a default using this command. See the **class** command to add a class. You can assign a context to one resource class only. An exception is that limits that are undefined in the member class are inherited from the default class; a context could be a member of a default plus another class.

Examples

This example shows how to assign a context to a class:

```
fwsm(config)# context intranet
fwsm(config-context)# member regulus
fwsm(config-context)#
```

Related Commands

Other Context Subconfiguration Commands

allocate-interface (context submode)
config-url (context submode)
limit-resource (class submode)

Other Related Commands

admin-context
changeto
class

clear context
show class
show context

mgcp

To configure additional support for the Media Gateway Control Protocol (MGCP) fixup (packet application inspection), use the **mgcp** command. To remove MGCP support, use the **no** form of this command.

[**no**] **mgcp call-agent** *ip_address group_id*

[**no**] **mgcp command-queue** *limit*

[**no**] **mgcp gateway** *ip_address group_id*

Syntax Description

call-agent *ip_address*	Specifies the IP address of the call agent.
command-queue *limit*	Specifies the maximum number of commands to queue; valid values are from 1 to 4294967295.
gateway *ip_address*	Specifies the IP address of the gateway.
group_id	Call agent group ID; valid values are from 0 to 4294967295.

Defaults

The MGCP command queue *limit* is 200.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **mgcp** command allows you to provide additional support for the MGCP fixup. The MGCP fixup is enabled with the **fixup protocol mgcp** command.

The **mgcp call-agent** command is used to specify a group of call agents that can manage one or more gateways. The call agent group information is used to open connections for the call agents in the group (other than the one to which the gateway sends a command) so that any of the call agents can send the response. Call agents with the same *group_id* belong to the same group. A call agent may belong to more than one group.

The **mgcp command-queue** command allows you to specify the maximum number of MGCP commands that are queued while waiting for a response. When the limit has been reached and a new command arrives, the command that has been in the queue for the longest time is removed.

The **mgcp gateway** command allows you to specify which group of call agents are managing a particular gateway. The IP address of the gateway is specified with the *ip_address* argument. The *group_id* argument must correspond with the *group_id* of the call agents that are managing the gateway. A gateway may belong to one group only.

Examples

This example shows how to limit the MGCP command queue to 150 commands, 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:

```
fwsm(config)# mgcp call-agent 10.10.11.5 101
fwsm(config)# mgcp call-agent 10.10.11.6 101
fwsm(config)# mgcp call-agent 10.10.11.7 102
fwsm(config)# mgcp call-agent 10.10.11.8 102
fwsm(config)# mgcp command-queue 150
fwsm(config)# mgcp gateway 10.10.10.115 101
fwsm(config)# mgcp gateway 10.10.10.116 102
fwsm(config)# mgcp gateway 10.10.10.117 102
```

Related Commands

clear mgcp
debug
fixup protocol
show conn
show mgcp
timeout

mkdir

To create a new directory, use the **mkdir** command.

mkdir [**/noconfirm**] [**disk:**] *path*

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	(Optional) Changes the current working directory.
path	Path for the new directory.

Defaults

If you do not specify a directory, the directory is changed to **disk:**.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If a directory with the same name already exists, then the new directory is not created. The **mkdir disk:** command prompts you to enter a directory name.

Examples

This example shows how to make a new directory:

```
fwsm(config)# mkdir disk:
Create directory filename [running-config]? my_context-configs
Created dir disk:my_context-configs
fwsm(config)# dir
Directory of disk:/
11     -rw-  1399        16:16:24 Mar 08 2005    old_running.cfg
12     -rw-  1242        16:16:26 Mar 08 2005    admin.cfg
30     drw-  0           18:24:50 Mar 10 2005    my-context-configs
60530688 bytes total (60342272 bytes free)
```

Related Commands

cd
copy disk
copy flash
copy ftp
dir
format
more
pwd
rename
rmdir
show file

mode

To change the FWSM to single context mode or multiple context mode, use the **mode** command.

mode {**single** | **multiple**}

Syntax Description

single	Sets the FWSM to the single context mode.
multiple	Sets the FWSM to the multiple context mode.

Defaults

The default setting depends on whether Cisco shipped the FWSM to you with the Security Context feature enabled (multiple context mode), or whether you are upgrading your FWSM (single context mode).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: System and Context

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is shown in privileged mode, but can only be run from the configuration mode. This command allows you to change the behavior of the FWSM and prompts you to reboot the module. By default, multiple mode allows you to use two contexts. To enable more than two contexts, you must enter an activation key (if it was not already entered by Cisco).

If you are changing from single context mode to multiple context mode, the FWSM converts the running configuration into two files: a new startup.cfg (in the Flash) that has the system configuration and admin.cfg (in the disk partition) that has the admin context. The original running configuration is saved as old_running.cfg (in disk). The original startup configuration is not saved.

If you convert from multiple context mode to single context mode, the startup configuration is not automatically converted back to the original running configuration. You must copy the backup version to the running and startup configurations. Because the system configuration does not have any network interfaces as part of its configuration, you must session into the FWSM from the switch to perform the copy as follows:

```
fwsm# copy disk:old_running.cfg running-config
fwsm# copy running-config startup-config
```

Examples

This example shows how to change the context mode:

```
FWSM(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
```

Related Commands

show mode

monitor-interface

To enable interface monitoring on a specific interface within a context, use the **monitor-interface** command.

[**no**] **monitor-interface** *interface_name*

Syntax Description

interface_name	Name of the interface being monitored.

Defaults

Not configured

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.
2.3(1)	Support for the Autostate feature was added on the FWSM.

Usage Guidelines

The number of interfaces that can be monitored for the FWSM is 250 per module. Hello messages are exchanged during every interface poll frequency time period between the FWSM failover pair. The failover interface poll time is 3 to 15 seconds. For example, if the poll time is set to 5 seconds, testing begins on an interface if 5 consecutive hellos are not heard on that interface (25 seconds).

Monitored failover interfaces can have the following status:

- Unknown—Initial status. This status can also mean the status cannot be determined.
- Normal—The interface is receiving traffic.
- Testing—Hello messages are not heard on the interface for five poll times.
- Link Down—The VLAN for the interface is shut down.
- No Link—VLANs for the interface are not configured.
- Failed—No traffic is received on the interface, yet traffic is heard on the peer interface.

Examples

This example shows how to start interface monitoring:

```
fwsm(config)# monitor-interface inside
```

Related Commands

clear failover
failover
failover interface ips
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
failover reset
show failover
show monitor-interface
write standby

more

To display the contents of a file, use the **more** command.

more [**/ascii**] || [**/binary**] [**disk:**] *path*

Syntax Description

/ascii	(Optional) Displays a binary file in binary mode and an ASCII file in binary mode.
/binary	(Optional) Displays any file in binary mode.
disk:	(Optional) Changes the current working directory.
path	Path for the new directory.

Defaults

ACSII mode

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **more disk:** command prompts you to enter a filename.

Examples

This example shows how to display the contents of a file named “test.cfg”:

```
fwsm(config)# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Jul 14 2003

FWSM Version 2.2(0)141
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
```

```
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no pdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@my_context.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

Related Commands

cd
copy disk
copy flash
copy running-config/copy startup-config
copy tftp
dir
format
mkdir
pwd
rename
rmdir
show file

mtu

To specify the maximum transmission unit (MTU) for an interface, use the **mtu** command. To reset the MTU block size to 1500 for Ethernet interfaces, use the **no** form of this command.

[**no**] **mtu** *interface_name bytes*

Syntax Description

interface_name	Internal or external network interface name.
bytes	Number of bytes in the MTU; valid values are from 64 to 65,535 bytes.

Defaults

bytes is 1500 for Ethernet interfaces.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **mtu** command allows you to set the data size that is sent on a connection. Data that is larger than the MTU value is fragmented before being sent.

The FWSM supports IP path MTU discovery (as defined in RFC 1191), which allows a host to dynamically discover and cope with the differences in the maximum allowable MTU size of the various links along the path. Sometimes, the FWSM cannot forward a datagram because the packet is larger than the MTU that you set for the interface, but the "don't fragment" (DF) bit is set. The network software sends a message to the sending host, alerting it to the problem. The host has to fragment packets for the destination so that they fit the smallest packet size of all the links along the path.

The default MTU is 1500 bytes in a block for Ethernet interfaces (which is also the maximum). This value is sufficient for most applications, but you can pick a lower number if network conditions require it.

When using the Layer 2 Timeline Protocol (L2TP), we recommend that you set the MTU size to 1380 to account for the L2TP header and IPSec header length.

Examples

This example shows how to specify the MTU for an interface:

```
fwsm/context_name(config)# mtu inside 8192
fwsm/context_name(config)# show mtu
fwsm/context_name(config)# mtu outside 1500
fwsm/context_name(config)# mtu inside 8192
```

Related Commands

show mtu

name

To associate a name with an IP address, use the **name** command. To enable the association, use the **names** command. To disable the use of the text names but not remove them from the configuration, use the **no** form of this command.

[**no**] **name** *ip_address name*

names

Syntax Description

ip_address	IP address of the host that is named.
name	Name assigned to the IP address.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Use the **names** command to enable association of a name with an IP address.

When defining the *name*, you can use characters a to z, A to Z, 0 to 9, a dash, and an underscore. The *name* cannot start with a number. If the name is over 16 characters, the **name** command fails.

The **name** command allows you to identify a host by a text name and map text strings to IP addresses. The **no names** command allows you to disable the use of the text names but does not remove them from the configuration. Use the **clear name** command to clear the list of names from the FWSM configuration.

You must first use the **names** command before you use the **name** command. Use the **name** command immediately after you use the **names** command and before you use the **write memory** command.

To disable displaying **name** values, use the **no names** command.

You can associate only one name with an IP address.

Both the **name** and **names** commands are saved in the configuration.

While the **name** command lets you assign a name to a network mask, no other FWSM command requiring a mask lets you use the name as a mask value. For example, this command is accepted:

```
fwsm/context_name(config)# name 255.255.255.0 class-C-mask
```

Note None of the commands in which a mask is required can process the "class-C-mask" as an accepted network mask.

Examples

This example shows that the **names** command allows you to enable use of the **name** command. The **name** command substitutes **fwsm_inside** for references to 192.168.42.3 and **fwsm_outside** for 209.165.201.3. You can use these names with the **ip address** commands when assigning IP addresses to the network interfaces. The **no names** command disables the **name** command values from displaying. Subsequent use of the **names** command again restores the **name** command value display.

```
fwsm(config)# names
fwsm(config)# name 192.168.42.3 fwsm_inside
fwsm(config)# name 209.165.201.3 fwsm_outside
fwsm(config)# ip address inside fwsm_inside 255.255.255.0
fwsm(config)# ip address outside fwsm_outside 255.255.255.224

fwsm(config)# show ip address
System IP Addresses:
    inside ip address fwsm_inside mask 255.255.255.0
    outside ip address fwsm_outside mask 255.255.255.224

fwsm(config)# no names
fwsm(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

fwsm(config)# names
fwsm(config)# show ip address
System IP Addresses:
    inside ip address fwsm_inside mask 255.255.255.0
    outside ip address fwsm_outside mask 255.255.255.224
```

Related Commands

clear name
show name

nameif

To name interfaces and assign the security level, use the **nameif** command.

no nameif *interface interface_name security_lvl*

no nameif *interface* [*interface_name*] [*security_lvl*]

Syntax Description

interface	VLAN name or mapped name.
interface_name	Name for the network interface; this name can have up to 48 characters.
security_lvl	Security level; valid values are from 0–100.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You cannot change the name of an interface; you can only change the security level. The interface identification is either vlan *num*, or for multiple mode, it is the mapped name that is configured with the **allocate interface** command. There is no hardware ID for the FWSM; only VLAN IDs are allowed.

Caution If you enter the **no nameif** command, all configurations that use that name are removed.

The security level between two interfaces determines the way the adaptive security algorithm is applied. A lower security_level interface is outside a higher level interface, and equivalent interfaces are outside each other. Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Software Configuration Guide* for more information about security levels.

Examples

This example shows a configuration in single mode:

```
fwsm(config)# nameif vlan18 perimeter1 sec50
fwsm(config)# nameif vlan23 perimeter2 sec20
```

This example shows a configuration in multiple mode:

```
fwsm(config-context)# allocate-interface vlan7 intf-out
fwsm(config-context)# allocate-interface vlan17 intf-in
```

```
fwsm(config-context)# allocate-interface vlan23 intf-dmz
fwsm(config-context)# changeto context_name
fwsm/context_name(config)# nameif intf-out outside security0
fwsm/context_name(config)# nameif intf-in inside security90
fwsm/context_name(config)# nameif intf-dmz dmz security50
```

Related Commands

allocate-interface (context submode)
interface
global
nat
static

names

To enable IP address to the name conversions that you can configure with the **name** command, use the **names** command. To disable address-to-name conversion, use the **no** form of this command.

[**no**] **names**

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to enable names:

```
fwsm(config)# names
```

Related Commands

clear name
name
show name
show names

nat

To associate a network with a pool of global IP addresses, use the **nat** command. To remove the **nat** command, use the **no** form of this command.

[**no**] **nat** *local_interface nat_id local_ip* [*mask* [**dns**] [**outside**] [[**tcp**] *tcp_max_conns* [*emb_limit*] [**norandomseq**]]] [**udp** *udp_max_conns*]

[**no**] **nat** *local_interface nat_id* **access-list** *access_list_name* [**dns**] [**outside**] [[**tcp**] *tcp_max_conns* [*emb_limit*] [**norandomseq**]]] [**udp** *udp_max_conns*]

Syntax Description

local_interface	Name of the network interface as specified by the **nameif** command through which the hosts or network that are designated by *local_ip* are accessed.
nat_id	ID of the group of host or networks; see the "Usage Guidelines" section for valid values.
local_ip	Internal network IP address to be translated.
mask	(Optional) IP netmask to apply to the *local_ip*.
dns	(Optional) Specifies to use the created translation to rewrite the DNS address record.
outside	(Optional) Specifies that the **nat** command apply to the outside interface address.
norandomseq	(Optional) Disables TCP Initial Sequence Number (ISN) randomization protection.
tcp	(Optional) Specifies that the maximum TCP connections and embryonic limit are set for the TCP protocol.
tcp_max_conns	(Optional) Maximum number of simultaneous connections that the *local_ip* hosts allow. Idle connections are closed after the time that is specified by the **timeout connection** command.
emb_limit	(Optional) Maximum number of embryonic connections per host.
udp	(Optional) Specifies a maximum number of UDP connection parameters that can be configured.
udp_max_conns	(Optional) Sets the maximum number of simultaneous UDP connections that the *local_ip* hosts are each allowed to use. Idle connections are closed after the time that is specified by the **timeout connection** command.
access-list *access_list_name*	Specifies the traffic to exempt from Network Address Translation (NAT) processing, based on the access list that is specified by *access_list_name*.

Defaults

The defaults are as follows:

- *emb_limit* is 0.
- **udp** is not required.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines

An embyonic connection is a connection request that has not finished the necessary handshake between source and destination.

The **nat** command allows you to enable or disable address translation for one or more internal addresses. Address translation occurs when a host starts an outbound connection and the IP addresses in the internal network are translated into global addresses. NAT allows your network to have any IP addressing scheme and the FWSM protects these addresses from visibility on the external network.

Note The number of address translations allowed is per each FWSM. The FWSM supports 2,048 address translations for the **nat** command, 1,051 address translations for the **global** command, and 2,048 address translations for the **static** command.The FWSM also supports up to 4,096 access control entries (ACEs) in ACLs used for policy NAT.

Note The FWSM does not support NAT with a Cisco CallManager inside the firewall with IP phones outside the firewall because NAT does not support TFTP messages.

The **outside** keyword lets you enable or disable address translation for the external addresses. For access control, IPSec, and AAA, use the real outside address.

Note Enabling outside Port Address Translation (PAT) can make the FWSM vulnerable to a flood DoS attack. We recommend that you restrict the address range specified with the **nat** *nat_id local_ip mask* **outside** command. In addition, you should set the connection limit to a value that accounts for the memory capacity of the FWSM. A PAT session is made up of a PAT xlate and an UDP or TCP connection. A PAT xlate consumes about 120 bytes and a TCP or UDP connection consumes 250 bytes.

The **nat** *interface_name* **0 access-list** *access_list_name* command allows you to exempt traffic that is matched by the **access-list** commands from the NAT services. The extent to which the inside hosts are accessible from the outside depends on the **access-list** commands that you use to permit inbound access. The *interface_name* is the higher security level interface name. The *access_list_name* is the name that you use to identify the **access-list** command.

Adding the **access-list** keyword changes the behavior of the **nat 0** command. Without the **access-list** keyword, the command is backward compatible with previous versions. The **nat 0** command disables NAT. Specifically, proxy ARPing for the IP addresses is disabled when you enter the **nat 0** command.

Note The access list that you specify with the **nat 0 access-list** command does not work with an **access-list** command that contains a port specification. The following sample commands will not work:

```
fwsm/context_name(config)# access-list no-nat permit tcp host xx.xx.xx.xx host
yy.yy.yy.yy
fwsm/context_name(config)# nat (inside) 0 access-list no-nat
```

After changing or removing the **nat** command, use the **clear xlate** command.

The connection limit lets you set the maximum number of outbound connections that can be started with the IP address criteria that you specify. This limit lets you prevent a type of attack where processes are started without being completed.

Use the **no nat** command to remove the **nat** command.

See Table 2-11 for a list of interface access commands. The security levels for the demilitarized zones are 40 for dmz1 and 60 for dmz2.

Table 2-11 Interface Access Commands by Interface

From This Interface	To This Interface	Use This Command	From This Interface	To This Interface	Use This Command
inside	outside	**nat**	dmz2	outside	**nat**
inside	dmz1	**nat**	dmz2	dmz1	**nat**
inside	dmz2	**nat**	dmz2	inside	**static**
dmz1	outside	**nat**	outside	dmz1	**static**
dmz1	dmz2	**static**	outside	dmz2	**static**
dmz1	inside	**static**	outside	inside	**static**

To obtain access from a higher security level interface to a lower security level interface, use the **nat** command. From a lower security level interface to a higher security level interface, use the **static** command.

Enable identity address translation with the **nat 0** command.The **nat 0** command requires that traffic initiates from an inside host. Use this command when you have IP addresses that are the same as those commands that are used on more than one interface. The extent to which the inside hosts are accessible from the outside depends on the **access-list** commands that permit inbound access.

Addresses on each interface must be on a different subnet.

Entering the **nat 0 10.2.3.0** command allows those IP addresses in the 10.2.3.0 net to appear on the outside without translation. All other hosts are translated depending on how their **nat** commands appear in the configuration.

Entering the **nat 1 0 0** command allows all outbound connections to pass through the FWSM with address translation. If you use the **nat (inside) 1 0 0** command, you can start connections on any interface with a lower security level on both the perimeter interfaces and the outside interface. With NAT, you must also use the **global** keyword to provide a pool of addresses through which translated connections pass. The NAT ID must be the same on the **nat** and **global** commands.

Entering the **nat 1 10.2.3.0** command allows only outbound connections originating from the inside host 10.2.3.0 to pass through the FWSM to go to their destinations with address translation.

When specifying the network mask for *local_ip*, you can use 0.0.0.0 to allow all outbound connections to translate with IP addresses from the global pool. The netmask 0.0.0.0 can be abbreviated as 0.

The *nat_id* is referenced by the **global** command to associate a global pool with the *local_ip*.

*nat_id v*alues can be 0, **0 access list** *access_list_name*, or any number from 1 to 256. A *nat_id* of 0 indicates that no address translation takes place for *local_ip*.

A *nat_id* of **0 access list** *access_list_name* specifies the traffic to exempt from NAT processing, based on the access list that is specified by the *access_list_name*. This command is useful in a VPN configuration where traffic between private networks should be exempted from NAT.

A *nat_id* that is a number from 1 to 256 specifies the inside hosts for dynamic address translation. The dynamic addresses are chosen from a global address pool that is created when you enter the **global** command. The *nat_id* number must match the *global_id* number of the global address pool that you want to use for dynamic address translation.

The *local_ip* determines the group of hosts or networks that are referred to by *nat_id.* You can use 0.0.0.0 to allow all hosts to start outbound connections. The 0.0.0.0 *local_ip* can be abbreviated as 0. An IP address not found in a more explicit *nat_id* group defaults to a less explicit or a **0** which indicates the least explicit.

Idle connections are closed after the idle timeout is specified by the **timeout conn** command.

In both the **nat** and **static** statements, the *udp_max_conn* field is applicable even when the TCP *max_conns* limit is not set, by using the keyword **udp**. This allows the two limits to be exclusively configured.

Examples

This example shows how to make the addresses visible from the outside network:

```
fwsm/context_name(config)# nat (inside) 0 209.165.201.0 255.255.255.224
fwsm/context_name(config)# static (inside, outside) 209.165.201.0 209.165.201.0 netmask
255.255.255.224
fwsm/context_name(config)# access-list acl_out permit host 10.0.0.1 209.165.201.0
255.255.255.224 eq ftp
fwsm/context_name(config)# access-group acl_out in interface outside

fwsm/context_name(config)# nat (inside) 0 209.165.202.128 255.255.255.224
fwsm/context_name(config)# static (inside, outside) 209.165.202.128 209.165.202.128
netmask 255.255.255.224
fwsm/context_name(config)# access-list acl_out permit tcp host 10.0.0.1 209.165.202.128
255.255.255.224 eq ftp
fwsm/context_name(config)# access-group acl_out in interface outside
…
```

This example shows how to use the **nat 0 access-list** command to permit access to internal host 10.1.1.15 through the inside interface, “inside,” to bypass NAT when connecting to outside host 10.2.1.3:

```
fwsm/context_name(config)# access-list no-nat permit ip host 10.1.1.15 host 10.2.1.3
fwsm/context_name(config)# nat (inside) 0 access-list no-nat
```

This command shows how to disable all NAT on the FWSM with three interfaces:

```
fwsm/context_name(config)# access-list all-ip-packet permit ip 0 0 0 0
fwsm/context_name(config)# nat (dmz) 0 access-list all-ip-packet
fwsm/context_name(config)# nat (inside) 0 access-list all-ip-packet
```

These examples show how to specify that all the hosts on the 10.0.0.0 and 3.3.3.0 inside networks can start outbound connections:

```
fwsm/context_name(config)# nat (inside) 1 10.0.0.0 255.0.0.0
fwsm/context_name(config)# global (outside) 1 209.165.201.25-209.165.201.27 netmask
255.255.255.224
fwsm/context_name(config)# global (outside) 1 209.165.201.30

fwsm/context_name(config)# nat (inside) 3 10.3.3.0 255.255.255.0
fwsm/context_name(config)# global (outside) 3 209.165.201.10-209.165.201.25 netmask
255.255.255.224
```

Related Commands

access-list deny-flow-max
clear nat
global
interface
nameif
show nat
static

no flashfs

To downgrade the file system information, use the **flashfs** command. To remove the file system information, use the **no** form of this command.

no flashfs

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear flashfs** command allows you to clear the file system part of the Flash partition in the FWSM. Versions 4.*n* cannot use the information in the file system; you need to clear the memory to let the earlier version operate correctly.

The **clear flashfs** command does not affect the configuration that is stored in the Flash partition.

Examples

This example shows how to write the file system to the Flash partition before downgrading to a lower version of software:

```
fwsm(config)# no flashfs
```

Related Commands

clear flashfs
show flashfs

object-group

To define object groups that you can use to optimize your configuration, use the **object-group** command. Use the **no** form of this command to remove object groups from the configuration.

[**no**] **object-group icmp-type** *obj_grp_id*

icmp-type group subcommands
description *description_text*
icmp-object *icmp_type*

[**no**] **object-group network** *obj_grp_id*

network group subcommands
description *description_text*
network-object host *host_addr* | *host_name*
network-object *net_addr netmask*
group-object

[**no**] **object-group protocol** *obj_grp_id*

protocol group subcommands
description *description_text*
protocol-object *protocol*

[**no**] **object-group service** *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

service group subcommands
description *description_text*
port-object range *begin_service end_service*
port-object eq *service*

Syntax Description

icmp-type	Defines a group of ICMP types such as echo and echo-reply. After entering the main **object-group icmp-type** command, add ICMP objects to the ICMP type group with the **icmp-object** and the **group-object** subcommand.
obj_grp_id	Object group (1 to 64 characters) and can be any combination of letters, digits, and the "_", "-", "." characters.
description *description_text*	Adds a description of up to 200 characters to an object-group.
icmp-object	Adds ICMP objects to an ICMP-type object group.
icmp_type	Decimal number or name of an ICMP type.
network	Defines a group of hosts or subnet IP addresses. After entering the main **object-group network** command, add network objects to the network group with the **network-object** and the **group-object** subcommand.
network-object	Adds network objects to a network object group.
host	Defines a host object.
host_addr	Host IP address or host name (if the host name is already defined using the **name** command).
host_name	Host name (if the host name is not defined using the **name** command.

net_addr	Network address; used with *netmask* to define a subnet object.
netmask	Netmask; used with *net_addr* to define a subnet object.
group-object	Adds the network object groups.
protocol	Defines a group of protocols such as TCP and UDP. After entering the main **object-group protocol** command, add protocol objects to the protocol group with the **protocol-object** and the **group-object** subcommand.
protocol-object	Adds the protocol objects to a protocol object group.
protocol	Protocol name or number.
service	Defines a group of TCP/UDP port specifications such as "eq smtp" and "range 2000 2010." After entering the main **object-group service** command, add port objects to the service group with the **port-object** and the **group-object** subcommand.
tcp	Specifies that the service group is used for TCP.
udp	Specifies that the service group is used for UDP.
tcp-udp	Specifies that the service group can be used for TCP and UDP.
port-object	**object-group service** subcommand used to add port objects to a service object group.
range	Specifies the range parameters.
begin_service	Specifies the decimal number or name of a TCP or UDP port that is the beginning value for a range of services.
end_service	Specifies the decimal number or name of a TCP or UDP port that is the ending value for a range of services.
eq *service*	Specifies the decimal number or name of a TCP or UDP port for a service object.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Objects such as hosts, protocols, or services can be grouped, and then you can issue a single command using the group name to apply to every item in the group.

When you define a group with the **object-group** command and then use any FWSM command, the command applies to every item in that group. This feature can significantly reduce your configuration size.

Once you define an object group, you must use the **object-group** keyword before the group name in all applicable FWSM commands as follows:

```
fwsm# show object-group group_name
```

where *group_name* is the name of the group.

This example shows the use of an object group once it is defined:

```
fwsm/context_name(config)# access-list access_list_name permit tcp any object-group
group_name
```

In addition, you can group the **access-list** command arguments as shown in Table 2-12.

Table 2-12 Individual Arguments and Object Group Replacements

Individual Arguments	Object Group Replacement
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

You can group commands hierarchically; an object group can be a member of another object group.

To use object groups, you must do the following:

- Use the **object-group** keyword before the object group name in all commands as follows:

  ```
  fwsm/context_name(config)# access-list acl permit tcp object-group remotes
  object-group locals object-group eng_svc
  ```

  where *remotes* and *locals* are sample object group names.

- The object group must be nonempty.
- You cannot remove or empty an object group if it is currently being used in a command.

After you enter a main **object-group** command, the command mode changes to its corresponding submode. The object group is defined in the submode. The active mode is indicated in the command prompt format. For example, the prompt in the configuration terminal mode appears as follows:

```
fwsm_name (config-type)#
```

where *fwsm_name* is the name of the FWSM.

However, when you enter the **object-group** command, the prompt appears as follows:

```
fwsm#_name (config-type)#
```

where *fwsm_name* is the name of the FWSM, and *type* is the object-group type.

Use the **exit**, **quit**, or any valid config-mode commands such as **access-list** to close an **object-group** submode and exit the **object-group** main command.

The **show object-group** command displays all defined object groups by their *grp_id* when the **show object-group id** *grp_id* command is entered, and by their group type when you enter the *show object-group grp_type* command. When you enter the **show object-group** comnmand without an argument, all defined object groups are shown.

Use the **no object-group** command to remove a group of previously defined **object-group** commands. Without an argument, the **clear object-group** command allows you to remove all defined object groups that are not being used in a command. The *grp_type* argument removes all defined object groups that are not being used in a command for that group type only.

See Table 2-13 for a listing of ICMP type numbers and names.

Table 2-13 ICMP Types

Number	ICMP Type Name
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**adress-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

You can use all other FWSM commands in submode, including the **show** and **clear** commands.

Subcommands appear indented when displayed or saved by the **show config**, **write**, or **config** commands.

Subcommands have the same command privilege level as the main command.

When you use more than one object group in an **access-list** command, the elements of all object groups that are used in the command are linked together, starting with the first group's elements with the second group's elements, then the first and second group's elements together with the third group's elements, and so on.

The starting position of the description text is the character right after the white space (a blank or a tab) following the **description** keyword.

Examples

This example shows how to use the **object-group icmp-type** submode to create a new icmp-type object group:

```
fwsm(config)# object-group icmp-type icmp-allowed
fwsm(config-icmp-type)# icmp-object echo
fwsm(config-icmp-type)# icmp-object time-exceeded
fwsm(config-icmp-type)# exit
```

This example shows how to use the **object-group network** subcommand to create a new network object group:

```
fwsm(config)# object-group network sjc_eng_ftp_servers
fwsm(config-network)# network-object host sjc.eng.ftp.servcers
fwsm(config-network)# network-object host 172.23.56.194
fwsm(config-network)# network-object 192.1.1.0 255.255.255.224
fwsm(config-network)# exit
```

This example shows how to use the **object-group network** subcommand to create a new network object group and map it to an existing object-group:

```
fwsm(config)# object-group network sjc_ftp_servers
fwsm(config-network)# network-object host sjc.ftp.servers
fwsm(config-network)# network-object host 172.23.56.195
fwsm(config-network)# network-object 193.1.1.0 255.255.255.224
fwsm(config-network)# group-object sjc_eng_ftp_servers
fwsm(config-network)# exit
```

This example shows how to use the **object-group protocol** submode to create a new protocol object group:

```
fwsm(config)# object-group protocol proto_grp_1
fwsm(config-protocol)# protocol-object udp
fwsm(config-protocol)# protocol-object ipsec
fwsm(config-protocol)# exit

fwsm(config)# object-group protocol proto_grp_2
fwsm(config-protocol)# protocol-object tcp
fwsm(config-protocol)# group-object proto_grp_1
fwsm(config-protocol)# exit
```

This example shows how to use the **object-group service** submode to create a new port (service) object group:

```
fwsm(config)# object-group service eng_service tcp
fwsm(config-service)# group-object eng_www_service
fwsm(config-service)# port-object eq ftp
fwsm(config-service)# port-object range 2000 2005
fwsm(config-service)# exit
```

This example shows how to add and remove a text description to an object group:

```
fwsm(config)# object-group protocol protos1
fwsm(config-protocol)# description This group of protocols is for our internal network

fwsm(config-protocol)# show object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

fwsmdocipsec1(config-protocol)# no description
fwsmdocipsec1(config-protocol)# show object-group id protos1
object-group protocol protos1
```

This example shows how to use the **group-object** submode to create a new object group that consists of previously defined objects:

```
fwsm(config)# object-group network host_grp_1
fwsm(config-network)# network-object host 192.168.1.1
fwsm(config-network)# network-object host 192.168.1.2
fwsm(config-network)# exit

fwsm(config)# object-group network host_grp_2
fwsm(config-network)# network-object host 172.23.56.1
```

```
fwsm(config-network)# network-object host 172.23.56.2
fwsm(config-network)# exit

fwsm(config)# object-group network all_hosts
fwsm(config-network)# group-object host_grp_1
fwsm(config-network)# group-object host_grp_2
fwsm(config-network)# exit

fwsm(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
fwsm(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
fwsm(config)# access-list all permit tcp object-group all_hosts any eq www
```

Without the **group-object** command, you need to define the *all_hosts* group to include all the IP addresses that have already been defined in *host_grp_1* and *host_grp_2*. With the **group-object** command, the duplicated definitions of the hosts are eliminated.

These examples show how to use object groups to simplify the access list configuration:

```
fwsm/context_name(config)# object-group network remote
fwsm/context_name(config-network)# network-object host kqk.suu.dri.ixx
fwsm/context_name(config-network)# network-object host kqk.suu.pyl.gnl

fwsm/context_name(config)# object-group network locals
fwsm/context_name(config-network)# network-object host 172.23.56.10
fwsm/context_name(config-network)# network-object host 172.23.56.20
fwsm/context_name(config-network)# network-object host 172.23.56.194
fwsm/context_name(config-network)# network-object host 172.23.56.195

fwsm/context_name(config)# object-group service eng_svc ftp
fwsm/context_name(config-service)# port-object eq www
fwsm/context_name(config-service)# port-object eq smtp
fwsm/context_name(config-service)# port-object range 25000 25100
```

This grouping enables the access list to be configured in 1 line instead of 24 lines, which would be needed if no grouping is used. Instead, with the grouping, the access list configuration is as follows:

```
fwsm/context_name(config)# access-list acl permit tcp object-group remote object-group
locals object-group eng_svc
```

Note The **show config** and **write** commands allow you to display the access list as configured with the object group names. The **show access-list** command displays the access list entries that are expanded out into individual entries without their object groupings.

Related Commands

clear object-group
show object-group

ospf (interface submode)

To configure interface-specific Open Shortest Path First (OSPF) parameters, use the **ospf** command in the interface submode. To return to the default setting, use the **no** form of this command.

ospf {**authentication** [**message-digest** | **null**]} | {**authentication-key** *password*} | {**cost** *interface_cost*} | {**database-filter all out**} | {**dead-interval** *seconds*} | {**hello-interval** *seconds*} | {**message-digest-key** *key-id* **md5** *key*} | {**mtu-ignore**} | {**priority** *number*} | {**retransmit-interval** *seconds*} | {**transmit-delay** *seconds*}

no ospf

Syntax Description

authentication	Specifies the authentication type for an interface.
message-digest	(Optional) Specifies to use OSPF message digest authentication.
null	(Optional) Specifies to not use OSPF authentication.
authentication-key *password*	Assigns an OSPF authentication password for use by neighboring routing devices.
cost *interface_cost*	Specifies the cost (a link-state metric) of sending a packet through an interface; valid values are from 0 to 255, expressed as the link-state metric.
database-filter all out	Filters out outgoing link-state advertisements (LSAs) to an OSPF interface.
dead-interval *seconds*	Sets the interval before declaring that a neighboring routing device is down if no hello packets are received; valid values are from 1 to 65535 seconds.
hello-interval *seconds*	Specifies the interval between hello packets that are sent on the interface; valid values are from 1 to 65535 seconds.
message-digest-key *key_id*	Enables the Message Digest 5 (MD5) authentication and specifies the numerical authentication key ID number; valid values are from 1 to 255.
md5 *key*	Alphanumeric password of up to 16 bytes.
mtu-ignore	Disables OSPF maximum transmission unit (MTU) mismatch detection on receiving database packets.
priority *number*	Specifies the priority of the router; valid values are from 0 to 255.
retransmit-interval *seconds*	Specifies the time between LSA retransmissions for adjacent routers belonging to the interface; valid values are from 1 to 65535 seconds.
transmit-delay *seconds*	Sets the estimated time that is required to send a link-state update packet on the interface; valid values are from 1 to 65535 seconds.

Defaults

The defaults are as follows:

- OSPF routing is disabled on the FWSM interfaces.
- **mtu-ignore** is enabled.
- **authentication** is **null** (no area authentication).
- **dead-interval** is four times the interval set by the **ospf hello-interval** command.

- **hello-interval** *seconds* is 10 seconds.
- **retransmit-interval** *seconds* is 5 seconds.
- **transmit-delay** *seconds* is 1 second.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **routing interface** command is the main command for all interface-specific OSPF interface mode commands. Enter this command with the name of the FWSM interface (*interface_name*) that you want to configure, and then proceed with interface-specific configuration through the **routing interface** subcommands.

Once you enter the **routing interface** command, the command prompt appears as (config-routing)#, indicating that you are in the submode.

The **show routing** command allows you to display the configuration for the interface specified.

ospf authentication

The **ospf authentication** [**message-digest | null**] subcommand allows you to specify the authentication type for an interface. To remove the authentication type for an interface, use the **no ospf authentication** [**message-digest | null**] subcommand. The default for authentication is **null**, which means that there is no authentication. The **null** subcommand overrides password or message digest authentication (if configured) for an OSPF area.

ospf authentication-key

The **ospf authentication-key** *password* subcommand allows you to assign a password to be used by neighboring routers that are using the OSPF simple password authentication. The *password* argument can be any continuous string of characters that can be entered from the keyboard up to 8 bytes.

The **no ospf authentication-key** subcommand allows you to remove a previously assigned OSPF password.

ospf cost

The **ospf cost** *interface_cost* subcommand allows you to explicitly specify the cost of sending a packet on an interface. The *interface_cost* parameter is an unsigned integer value from 0 to 255.

The **no ospf cost** subcommand allows you to reset the path cost to the default value.

ospf database-filter all out

The **ospf database-filter** subcommand allows you to filter outgoing link-state advertisements (LSAs) to an OSPF interface. The **no ospf database-filter all out** subcommand allows you to restore the forwarding of LSAs to the interface.

ospf dead-interval

The **ospf dead-interval** *seconds* subcommand allows you to set the dead interval before neighbors to declare the router down (the length of time during which no hello packets are seen). *seconds* specifies the dead interval and must be the same for all nodes on the network. The default for *seconds* is four times the interval set by the **ospf hello-interval** command from 1 to 65535. The **no ospf dead-interval** subcommand allows you to return to the default interval value.

ospf hello-interval

The **ospf hello-interval** *seconds* subcommand allows you to specify the interval between hello packets that the FWSM sends on the interface. The **no ospf hello-interval** subcommand allows you to return to the default intervalt. The default is 10 seconds with a range from 1 to 65535.

ospf mtu-ignore

The **ospf mtu-ignore** subcommand allows you to disable OSPF MTU mismatch detection on receiving DBD packets and is enabled by default.

ospf message-digest-key *key_id* md5 *key*

The **ospf message-digest-key** *key_id* **md5** *key* subcommand allows you to enable OSPF Message Digest 5 (MD5) authentication. The **no ospf message-digest-key** *key_id* **md5** *key* subcommand allows you to remove an old MD5 key. *key_id* is a numerical identifier from 1 to 255 for the authentication key. *key* is an alphanumeric password of up to 16 bytes. White space characters, such as a tab or space, are not supported. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

ospf priority

The **ospf priority** *number* subcommand allows you to set the router priority, which helps determine the designated router for this network. The **no ospf priority** *number* subcommand allows you to return to the default value.

ospf retransmit-interval

The **ospf retransmit-interval** *seconds* subcommand allows you to specify the time between LSA retransmissions for adjacencies belonging to the interface. The **no ospf retransmit-interval** subcommand allows you to return to the default value. The default value is 5 seconds with a range from 1 to 65535.

ospf transmit-delay

The **ospf transmit-delay** *seconds* subcommand allows you to set the estimated time required to send a link-state update packet on the interface. The **no ospf transmit-delay** subcommand allows you to return to the default value. The default value is 1 second with a range from 1 to 65535.

Examples

This example shows how to enter the submode on the outside interface of the FWSM (needed to configure OSPF routing):

```
fwsm(config)# routing interface outside
```

In the routing submode, the command prompt appears as "(config-routing)#."

This example shows the configuration for two concurrently running OSPF processes, with the IDs 5 and 12, on the outside interface of the firewall:

```
fwsm(config)# routing interface
fwsm(config)# show ospf

 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0

 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

This example shows how to change the retransmit interval to 15 seconds:

```
fwsm(config-interface)# ospf retransmit-interval 15
```

Related Commands

routing interface
show routing

pager

To enable screen paging, use the **pager** command. To disable screen paging and let the output display without interruption, use the **no** form of this command.

[**no**] **pager** [**lines** *lines*]

Syntax Description

lines *lines*	(Optional) Specifies the number of lines before the "---more---" prompt appears; valid values are from 1 to 25.

Defaults

number is 24.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you set the **pager lines** command to a value and want to revert back to the default, enter the **pager** command without keywords or arguments. This command is session based. If the pager value is changed in a session, the value is not changed globally for other sessions. Use the **pager 0** command to disable paging.

When you enable paging, the "---more---" prompt appears. The "---more---" prompt uses syntax that is similar to the UNIX **more** command as follows:

- To display another screenful, press the **Space** bar.
- To display the next line, press the **Enter** key.
- To return to the command line, press the **q** key.

Examples

This example shows how to enable screen paging:

```
fwsm(config)# pager lines 2
fwsm(config)# ping inside 10.0.0.42
        10.0.0.42 NO response received -- 1010ms
        10.0.0.42 NO response received -- 1000ms
<--- more --->
```

Related Commands

clear pager
show pager

password/passwd

To set the password for Telnet access to the FWSM console, use the **password** command.

{**password** | **passwd**} *password* [**encrypted**]

Syntax Description

password	Case-sensitive password of up to 16 alphanumeric and special characters.
encrypted	(Optional) Specifies that the password that you entered is already encrypted.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuraton mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **password/passwd** command allows you to set a password for Telnet access to the FWSM console. The **passwd** keyword is also accepted as a shortened form of **password**. Additionally, the FWSM configuration displays the password using the short form, **passwd**.

Any character can be used in the password except a question mark and a space.The *password* that you specify with the **encrypted** keyword must be 16 characters.

An empty password is changed into an encrypted string. However, any use of the **write** command displays or writes the passwords in encrypted form. Once passwords are encrypted, they are not reversible back to plain text.

Note Write down the new password and store it in a manner consistent with your site's security policy. Once you change this password, you cannot see it again.

Examples

This example shows how to set the password for Telnet access to the FWSM console:

```
fwsm(config)# password watag00s1am
fwsm(config)# show password
passwd jMorNbK0514fadBh encrypted
```

Related Commands

clear password
enable
show password/passwd
telnet

pdm

To configure the support communication between the FWSM and a browser running the PDM, use the **pdm** command.

pdm disconnect *session_id*

[**no**] **pdm history enable**

pdm history [**view** {**all | 12h | 5d | 60m | 10m**}] [**snapshot**] [**feature** {**all | blocks | cpu | failover | ids | interface** *interface_name* **| memory | perfmon | xlates**}] [**pdmclient**]

pdm group *real_group_name associated_intf_name*

pdm group *ref_group_name ref_intf_name* **reference** *real_group_name*

pdm location *ip_address netmask interface_name*

pdm logging [*level* [*messages*]]

Syntax Description

disconnect *session_id*	Disconnects the specified PDM session from the FWSM.
history enable	Enables PDM data sampling.
view *type*	(Optional) Specifies the PDM history view to display; valid values for the type argument are 12 hours (**12h**), 5 days (**5d**), 60 minutes (**60m**), 10 minutes (**10m**), or **all** history contents in the PDM history buffer.
snapshot	(Optional) Displays only the last PDM history data point.
feature	(Optional) Specifies to display the history for a single feature.
all	(Optional) Displays the history for all the features.
blocks	(Optional) Displays the blocks used for the feature.
cpu	(Optional) Displays the history for CPU usage.
failover	(Optional) Displays the history for failover.
ids	(Optional) Displays the history for the Intrusion Detection System.
interface *interface_name*	(Optional) Specifies the interface name on which the PDM resides.
memory	(Optional) Displays the history for the memory; similar to the output of the **show memory** command.
perfmon	(Optional) Displays the history for performance.
xlates	(Optional) Displays the history for translation slot information.
pdmclient	(Optional) Displays the PDM history in PDM-display format.
real_group_name	Name of a PDM object group that contains real IP addresses.
associated_intf_name	Name of the interface to which the specified object group is associated.
ref_group_name	Name of an object group that contains the network address-translated IP addresses of the object group specified by *real_group_name*.
ref_intf_name	Name of the interface from which the destination IP address of the inbound traffic is network address translated.
reference	Associates an object group that contains real IP addresses to an object group that contains NAT IP addresses.

ip_address	Host or network on which the PDM resides.
netmask	Network mask for the **pdm location** *ip_address*.
location	Associates an interface with an IP address on which PDM resides.
logging	Specifies the type and number of syslog messages that are displayed through the PDM **syslog** keyword.
level	(Optional) Priority level of syslog messages that are displayed in the PDM **syslog** keyword.
messages	(Optional) Maximum number of messages that are stored in the PDM buffer before the buffer discards the old messages.

Defaults

The defaults are as follows:

- The PDM syslog *level* is 0.
- The logging *messages* is 100.
- The maximum is 512.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	The PDM software version 2.2 was used to configure the FWSM release 1.1(1). In this release, the PDM has been replaced by the Firewall Device Manager (FDM).

Usage Guidelines

The *associated_intf_name* name is defined by the **nameif** command.

The *ref_intf_name* name is defined by the **nameif** command.

The **pdm location** command is an internal PDM command.

Once the message buffer exceeds the specified *message*, old messages are discarded.

The **pdm history enable** command allows you to enable the PDM data sampling. If not specified, the history for all features is displayed. PDM data sampling takes a data sample and stores the sample data to the PDM history buffer. The **no** form of this command disables PDM data sampling.

The **pdm disconnect** command and the **show pdm sessions** commands are accessible through the FWSM command-line interface.

The **failover** keyword history display is similar to the output of the **show failover** command.

The **memory** keyword history display is similar to the output of the **show perfmon** command.

The **xlates** keyword history display is similar to the output of the **show xlate** command.

The **clear pdm**, **pdm group**, **pdm history**, **pdm location**, and **pdm logging** commands may appear in your configuration, but they are designed to work as internal PDM-to-FWSM commands that are accessible only to the PDM.

You can only associate one interface to an *ip_address*/*netmask* pair when you enter the **pdm location** command. Specifying a new pair replaces the old definition.

Examples

This example shows how to report the last data point in PDM-display format:

```
fwsm(config)# pdm history enable
fwsm(config)# show pdm history view 10m snapshot pdmclient
INTERFACE|outside|up|IBC|0|OBC|1088|IPC|0|OPC|0|IBR|17|OBR|0|IPR|0|OPR|0|IERR|1|NB|0|RB|0|
RNT|0|GNT|0|CRC|0|FRM|0|OR|0|UR|0|OERR|0|COLL|0|LCOLL|0|RST|0|DEF|0|LCR|0:FWSMoutsideINTER
FACE:METRIC_HISTORY|SNAP|IBR|VIEW|10|1952|METRIC_HISTORY|SNAP|OBR|VIEW|10|64|METRIC_HISTOR
Y|SNAP|IPR|VIEW|10|17|METRIC_HISTORY|SNAP|OPR|VIEW|10|1|METRIC_HISTORY|SNAP|IERR|VIEW|10|0
|METRIC_HISTORY|SNAP|OERR|VIEW|10|0|:FWSMinsideINTERFACE:METRIC_HISTORY|SNAP|IBR|VIEW|10|0
|METRIC_HISTORY|SNAP|OBR|VIEW|10|64|METRIC_HISTORY|SNAP|IPR|VIEW|10|0|METRIC_HISTORY|SNAP|
OPR|VIEW|10|1|METRIC_HISTORY|SNAP|IERR|VIEW|10|0|METRIC_HISTORY|SNAP|OERR|VIEW|10|0|:FWSMS
YS:METRIC_HISTORY|SNAP|MEM|VIEW|10|52662272|METRIC_HISTORY|SNAP|BLK4|VIEW|10|1600|METRIC_H
ISTORY|SNAP|BLK80|VIEW|10|400|METRIC_HISTORY|SNAP|BLK256|VIEW|10|998|METRIC_HISTORY|SNAP|B
LK1550|VIEW|10|676|METRIC_HISTORY|SNAP|XLATES|VIEW|10|0|METRIC_HISTORY|SNAP|CONNS|VIEW|10|
0|METRIC_HISTORY|SNAP|TCPCONNS|VIEW|10|0|METRIC_HISTORY|SNAP|UDPCONNS|VIEW|10|0|METRIC_HIS
TORY|SNAP|URLS|VIEW|10|0|METRIC_HISTORY|SNAP|WEBSNS|VIEW|10|0|METRIC_HISTORY|SNAP|TCPFIXUP
S|VIEW|10|0|METRIC_HISTORY|SNAP|TCPINTERCEPTS|VIEW|10|0|METRIC_HISTORY|SNAP|HTTPFIXUPS|VIE
W|10|0|METRIC_HISTORY|SNAP|FTPFIXUPS|VIEW|10|0|METRIC_HISTORY|SNAP|AAAAUTHENUPS|VIEW|10|0|
METRIC_HISTORY|SNAP|AAAAUTHORUPS|VIEW|10|0|METRIC_HISTORY|SNAP|AAAACCOUNTS|VIEW|10|0|
```

This example shows how to report the data formatted for the FWSM CLI:

```
fwsm(config)# pdm history enable
fwsm(config)# show pdm history view 10m snapshot
Available 4 byte Blocks:  [  10s] : 1600
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 400
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 500
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 931
Used 1550 byte Blocks:  [  10s] : 385
Available 1552 byte Blocks:  [  10s] : 0
Used 1552 byte Blocks:  [  10s] : 0
Available 2560 byte Blocks:  [  10s] : 0
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 0
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 0
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 0
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 0
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 0
IP Options Bad:  [  10s] : 0
Record Packet Route:  [  10s] : 0
IP Options Timestamp:  [  10s] : 0
Provide s,c,h,tcc:  [  10s] : 0
Loose Source Route:  [  10s] : 0
SATNET ID:  [  10s] : 0
Strict Source Route:  [  10s] : 0
IP Fragment Attack:  [  10s] : 0
Impossible IP Attack:  [  10s] : 0
IP Teardrop:  [  10s] : 0
```

```
ICMP Echo Reply:  [  10s] : 0
ICMP Unreachable:  [  10s] : 0
ICMP Source Quench:  [  10s] : 0
ICMP Redirect:  [  10s] : 0
ICMP Echo Request:  [  10s] : 0
ICMP Time Exceeded:  [  10s] : 0
ICMP Parameter Problem:  [  10s] : 0
ICMP Time Request:  [  10s] : 0
ICMP Time Reply:  [  10s] : 0
ICMP Info Request:  [  10s] : 0
ICMP Info Reply:  [  10s] : 0
ICMP Mask Request:  [  10s] : 0
ICMP Mask Reply:  [  10s] : 0
Fragmented ICMP:  [  10s] : 0
Large ICMP:  [  10s] : 0
Ping of Death:  [  10s] : 0
No Flags:  [  10s] : 0
SYN & FIN Only:  [  10s] : 0
FIN Only:  [  10s] : 0
FTP Improper Address:  [  10s] : 0
FTP Improper Port:  [  10s] : 0
Bomb:  [  10s] : 0
Snork:  [  10s] : 0
Chargen:  [  10s] : 0
DNS Host Info:  [  10s] : 0
DNS Zone Transfer:  [  10s] : 0
DNS Zone Transfer High Port:  [  10s] : 0
DNS All Records:  [  10s] : 0
Port Registration:  [  10s] : 0
Port Unregistration:  [  10s] : 0
RPC Dump:  [  10s] : 0
Proxied RPC:  [  10s] : 0
ypserv Portmap Request:  [  10s] : 0
ypbind Portmap Request:  [  10s] : 0
yppasswd Portmap Request:  [  10s] : 0
ypupdated Portmap Request:  [  10s] : 0
ypxfrd Portmap Request:  [  10s] : 0
mountd Portmap Request:  [  10s] : 0
rexd Portmap Request:  [  10s] : 0
rexd Attempt:  [  10s] : 0
statd Buffer Overflow:  [  10s] : 0
Input KByte Count:  [  10s] : 41804
Output KByte Count:  [  10s] : 526456
Input KPacket Count:  [  10s] : 364
Output KPacket Count:  [  10s] : 450
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 90076
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 8895
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 3138
Lost Carrier:  [  10s] : 0
```

```
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Input KByte Count:  [  10s] : 61835
Output KByte Count:  [  10s] : 26722
Input KPacket Count:  [  10s] : 442
Output KPacket Count:  [  10s] : 418
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 308607
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 2
Lost Carrier:  [  10s] : 707
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Available Memory:  [  10s] : 45293568
Used Memory:  [  10s] : 21815296
Xlate Count:  [  10s] : 0
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
PPTP Sessions:  [  10s] : 0
PPTP Tunnels:  [  10s] : 0
```

Related Commands

clear pdm
fixup protocol
setup
show pdm

perfmon

To display performance information, use the **perfmon** command.

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**}

Syntax Description

verbose	Displays performance monitor information at the FWSM console.
interval *seconds*	Specifies the number of seconds before the performance display is refreshed on the console.
quiet	Disables the performance monitor displays.
settings	Displays the interval and whether it is quiet or verbose.

Defaults

The *seconds* is 120 seconds.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **perfmon** command allows you to monitor the performance of the FWSM. Use the **show perfmon** command to display the information immediately. Use the **perfmon verbose** command to display the information every 2 minutes continuously. Use the **perfmon interval** *seconds* command with the **perfmon verbose** command to display the information continuously every number of seconds that you specify.

An example of the performance information is displayed as follows:

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s

AAA Author	9/s	5/s
AAA Account	3/s	3/s

This information lists the number of translations, connections, Websense requests, address translations (called “fixups”), and AAA transactions that occur each second.

Examples

This example shows how to display the performance monitor statistics every 30 seconds on the FWSM console:

```
fwsm/context_name(config)# perfmon interval 120
fwsm/context_name(config)# perfmon quiet
fwsm/context_name(config)# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands

show perfmon

ping

To determine if other IP addresses are visible from the FWSM, use the **ping** command.

ping [*interface_name*] *ip_address*

Syntax Description

interface_name	(Optional) Internal or external network interface name.
ip_address	IP address of a host on the inside or outside networks.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **ping** command allows you to determine if the FWSM has connectivity or if a host is available on the network. If the FWSM is connected, you should also ensure that the **icmp permit any** *interface* command is configured. This configuration is required to allow the FWSM to respond and accept these messages. The command output shows if the response was received. If a host is not responding, when you enter the **ping** command, you see the display "NO response received." Use the **show interface** command to ensure that the FWSM is connected to the network and is passing traffic.

The address of the specified *interface_name* is used as the source address of the ping.

If you want internal hosts to ping external hosts, you must create an ICMP **access-list** command for an echo reply; for example, to give ping access to all hosts, use the **access-list** *acl_grp* **permit icmp any any** command and bind the **access-list** command to the interface that you want to test using the **access-group** command.

If you are pinging through the FWSM between hosts or routers, but the pings are not successful, use the **debug icmp trace** command to monitor the success of the ping. Pings are successful when they are both inbound and outbound.

The FWSM **ping** command does not require an interface name. If you do not specify an interface name, the FWSM checks the routing table to find the address that you specify. You can specify an interface name to indicate through which interface the ICMP echo requests are sent.

Examples

This example shows how to determine if other IP addresses are visible from the FWSM:

```
fwsm(config)# ping 192.168.42.54
fwsm(config)# ping 10.0.0.1
```

```
10.0.0.1 response received -- 10ms
10.0.0.1 response received -- 10ms
10.0.0.1 response received -- 0ms
```

You can enter the command specifying the interface as follows:

```
fwsm(config)# ping outside 10.0.0.1
10.0.0.1 response received -- 10ms
10.0.0.1 response received -- 10ms
10.0.0.1 response received -- 0ms
```

Related Commands

icmp
show interface

privilege

To configure the command privilege levels, use the **privilege** command. To disallow the configuration, use the **no** form of this command.

[**no**] **privilege** [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

Syntax Description

show	(Optional) Sets the privilege level for the **show** command corresponding to the command specified.
clear	(Optional) Sets the privilege level for the **clear** command corresponding to the command specified.
configure	(Optional) Sets the privilege level for the **configure** command corresponding to the command specified.
level *level*	Specifies the privilege level; valid values are from 0 to 15.
mode enable	(Optional) Indicates that the level is for the enable mode of the command.
mode configure	(Optional) Indicates that the level is for the configure mode of the command.
command *command*	Specifies the command on which to set the privilege level.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **privilege** command allows you to set user-defined privilege levels for the FWSM commands. This command is useful for setting different privilege levels for related configuration, **show** commands, and **clear** commands. Make sure that you verify privilege level changes in your commands with your security policies before using the new privilege levels.

When commands and users have privilege levels set, the two are compared to determine if a given user can execute a given command. If the user's privilege level is lower than the privilege level of the command, the user is prevented from executing the command.

To change between privilege levels, use the **login** command to access another privilege level and the appropriate **logout**, **exit**, or **quit** command to exit that level.

The **mode enable** and **mode configure** keywords are for commands with both enable and configure modes.

Lower privilege level numbers are lower privilege levels.

Note The **aaa authentication** and **aaa authorization** commands need to include any new privilege levels that you define before you can use them in your AAA server configuration.

Examples

This example shows how to set the privilege level "5" for an individual user as follows:

```
username intern1 password pass1 privilege 5
```

This example shows how to define a set of **show** commands with the privilege level "5" as follows:

```
fwsm(config)# privilege show level 5 command alias
fwsm(config)# privilege show level 5 command arp
fwsm(config)# privilege show level 5 command auth-prompt
fwsm(config)# privilege show level 5 command blocks
```

This example shows how to apply privilege level 11 to a complete AAA authorization configuration:

```
fwsm(config)# privilege configure level 11 command aaa
fwsm(config)# privilege configure level 11 command aaa-server
fwsm(config)# privilege configure level 11 command access-group
fwsm(config)# privilege configure level 11 command access-list
fwsm(config)# privilege configure level 11 command activation-key
fwsm(config)# privilege configure level 11 command age
fwsm(config)# privilege configure level 11 command alias
```

Related Commands

aaa authentication
clear privilege
login
object-group
show curpriv
show privilege
username

pwd

To display the current working directory, use the **pwd** command.

pwd

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Fiewall Mode: Routed and Transparent

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the current working directory:

```
fwsm(config)# pwd
disk:
```

Related Commands

cd
copy disk
copy flash
copy running-config/copy startup-config
copy tftp
dir
format
mkdir
more
rename
rmdir
show file

quit

To exit the current privilege level or mode, use the **quit** command.

quit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: System Context Command Line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You may also use the key sequence **^Z** to exit.

Examples

This example shows how to use the **quit** command:

```
fwsm(config)# quit
fwsm# quit
fwsm>
```

Related Commands

exit

redistribute (OSPF submode)

To configure redistribution between the Open Shortest Path First (OSPF) processes according to the specified parameters, use the **redistribute** command. To remove redistribution configurations, use the **no** form of this command.

redistribute {**static | connected**} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

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

Syntax Description

static	Specifies the static interface.
connected	Specifies the connected interface.
metric *metric_value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type *metric_type*	(Optional) Specifies the OSPF metric type; valid values are **type-1**, **type-2**, **internal**, or **external**.
route-map *map_name*	(Optional) Name of the route map to apply.
tag *tag_value*	(Optional) Specifies the value to match for controlling redistribution with route maps.
subnets	(Optional) Specifies for redistributing routes into OSPF and scopes the redistribution for the specified protocol.
ospf *pid*	Specifies an internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
match	(Optional) Specifies the conditions for redistributing routes from one routing protocol into another.
internal *type*	Specifies OSPF metric routes that are internal to a specified autonomous system; valid values are **1** or **2**.
external *type*	Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are **1** or **2**.
nssa-external *type*	Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are **1** or **2**.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The**show router** **ospf** command allows you to display the configured **router ospf** subcommands.

You assign the *pid* locally on the FWSM; it can be from 1 to 65535. You must assign a unique value for each OSPF routing process.

Examples

This example shows how to configure redistribution between the OSPF processes according to the specified parameters:

```
fwsm(config)# router ospf 1
fwsm(config-router)# redistribute static
% Only classful networks will be redistributed
fwsm(config-router)#
```

Related Commands

router ospf
show ip ospf
show redistribute

reload

To reboot and reload the configuration, use the **reload** command..

reload [**noconfirm**]

Syntax Description

noconfirm	(Optional) Permits the FWSM to reload without user confirmation.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **reload** command allows you to reboot the FWSM and reload the configuration from a bootable floppy disk. If a disk is not present, it allows you to reboot and reload from the Flash partition.

The FWSM does not accept abbreviations for **noconfirm**.

You are prompted for confirmation before the "Proceed with reload?" message displays. Only a response of **y** causes the reboot to occur.

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:

```
fwsm(config)# reload
Proceed with reload?  [confirm] y

Rebooting...

fwsm Bios V2.7
...
```

Related Commands

shutdown

rename

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

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

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	(Optional) Specifies the location of the source file.
source-path	(Optional) Path of the source file.
disk:	(Optional) Specifies the location of the destination file.
destination-path	(Optional) Path of the destination file.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

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

Examples

This example shows how to show the contents of a file named test1:

```
fwsm(config)# rename disk: disk:
Source filename [running-config]? test
Destination filename [n]? test1
```

Related Commands

cd
copy disk
copy flash
copy startup-config
copy tftp
dir
format
mkdir
more
pwd
rmdir
show file

resource acl-partition

To partition the ACL memory into a specified number of partitions, use the **resource acl-partition** command. To partition the ACL memory into the default of 12 memory partitions, use the **no** form of this command.

[**no**] **resource acl-partition** *number-of-partitions*

Syntax Description

number-of-partitions	Specifies the context.

Defaults

Twelve ACL memory partitions.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command prompts you for a reboot if you run the command after the creation of the first context. The change will not take place until the next reboot.

When you enter the **resource acl-partition X** command, the ACL memory is partitioned into X+1 partitions. The extra 1 is for backup. This command prompts you for a reboot if the command is entered after the creation of the first context. In this case, the change does not take place until the next reboot.

You must reboot the module before the changes will take place. In a failover setup you must reload both the blades together. There will be some network downtime due to both blades rebooting

The **no resource acl-partition X** command partitions the ACL memory into the default of 12 partitions.

The following caveats apply to this command:

- resource acl-partition <X> will not take effect until the user enters the **write memory** command and reboots the module.
- If you are using a failover configuration, then the recommended command sequence is as follows:

  On the active module, the command sequence is as follows:

```
resource acl-partition X
write mem
reload
```

  On the standby module, the command sequence is as follows:

```
reload
```

- The **resource acl-partition** command is available only in multiple mode, not in single mode.

Note The active and standby modules must be rebooted together. Traffic loss occurs because both the active and the standby modules are down at the same time.

- The maximum number for rules of each type is a function of the number of partitions.

  For example, when the number of partitions is 12, the following apply:

  Max Filter rules—606

  Max Established rules—121

  Max AAA rules—1213

  Max ACL rules—9704

  Max Console Access rules—363

  Max PolicyNAT rules—606

Examples

The ACL partition 0 is nonexclusive by “bandn,” and “borders.” The remaining contexts share ACL partition 1.

This example shows how ACL partition 0 is given to “bandn” exclusively and ACL partition 1 is given to borders exclusively. The remaining customers are distributed among partitions 2 and 3 in a round-robin sequence.

```
FWSM/system # resource acl-partition 4
FWSM/system # context bandn
FWSM/system # allocate-acl-partition 0
FWSM/system # context borders
FWSM/system # allocate-acl-partition 1
FWSM/system # context mompopa
FWSM/system # context mompopb
FWSM/system # context mompopc
FWSM/system # context mompopd
```

To verify the current mapping of contexts to acl partitions, use the following command.

```
FWSM(config)# show resource acl-partition
Total number of configured partitions = 2
Partition# 0
        Mode                        : exclusive
        List of Contexts          : bandn, borders
        Number of contexts    : 2(RefCount:2)
        Number of rules           : 0(Max:53087)
Partition# 1
        Mode                        : non-exclusive
        List of Contexts          : admin, momandpopA, momandpopB, momandpopC
                                    momandpopD
        Number of contexts    : 5(RefCount:5)
        Number of rules           : 6(Max:53087)
FWSM(config)#
```

Related Commands

allocate-acl-partition (context submode)
clear resource usage
resource-manager

show resource allocation
show resource types
show resource usage

resource-manager

To assign the contexts to the memory pools, use the **resource-manager** command.

resource-manager allocate-resource acl-memory-pool [**num**]

Syntax Description

allocate-resource	Specifies the context.
acl-memory-pool	Specifies the ACL memory pool.
num	(Optional) Numbers the memory pool; the range is from 1 to 12.

Defaults

Twelve ACL memory pools.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This feature allows you to manage memory resources by specifying up to 12 memory pools per context. The contexts are assigned to ACL memory pools using the round-robin algorithm. You can assign the contexts to the specific memory pools to control how many and which contexts share the same ACL memory pool. You can also specify which contexts have pools that are assigned to them and how much ACL memory is available to each context.

Examples

This example shows how to assign contexts to memory pools:

```
fwsm(config)# resource-manager allocate-resource acl-memory-pool 1
```

rip

To enable and change the Routing Information Protocol (RIP) settings, use the **rip** command. To disable the FWSM IP routing table updates, use the **no** form of this command.

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

no rip *interface_name*

Syntax Description

interface_name	Internal or external network interface name.
default	Broadcasts a default route on the interface.
passive	Enables passive RIP on the interface.
version	(Optional) Specifies the RIP version; valid values are **1** and **2**.
authentication	(Optional) Enables RIP version 2 authentication.
text	(Optional) Clear text (not recommended) for sending RIP updates.
md5	(Optional) MD5 encryption for sending RIP updates.
key	(Optional) Key to encrypt RIP updates.
key_id	(Optional) Key identification value; valid values are from 1 to 255.

Defaults

Enabled

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **rip** command allows you to enable IP routing table updates from received RIP broadcasts. If you specify RIP version 2, you can encrypt RIP updates using MD5 encryption. The **version 1** keyword provides backward compatibility with the older version.

Ensure that the *key* and *key_id* arguments are the same arguments that are used on any other device in your network that makes RIP version 2 updates. The *key* is a text string of up to 16 characters.

The FWSM cannot pass RIP updates between interfaces.

You configure RIP version 2 in passive mode. The FWSM listens for RIP routing broadcasts and uses that information to populate its routing tables. The FWSM accepts RIP version 2 multicast updates with an IP destination of 224.0.0.9. For RIP version 2 default mode, the FWSM transmits default route updates using an IP destination of 224.0.0.9. Configuring RIP version 2 registers the multicast address 224.0.0.9 so that the interface can accept multicast RIP version 2 updates.

Only Intel 10/100 and Gigabit interfaces support multicasting.

When you remove the RIP version 2 commands for an interface, you are unregistering the multicast address from the interface card.

Examples

This example shows how to sample output from the version 1 **show rip** and **rip inside default** commands:

```
fwsm/context_name(config)# show rip
rip outside passive
no rip outside default
rip inside passive
no rip inside default

fwsm/context_name(config)# rip inside default
fwsm/context_name(config)# show rip
rip outside passive
no rip outside default
rip inside passive
rip inside default
```

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

- Enable version 2 passive 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.

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

fwsm/context_name(config)# show 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
```

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

```
fwsm/context_name(config)# rip out default version 2 authentication text thisisakey 3
fwsm/context_name(config)# show rip
rip outside default version 2 authentication text thisisakey 3
```

Related Commands

clear rip
show rip

rmdir

To remove the existing directory, use the **rmdir** command.

rmdir [**/noconfirm**] [**disk:**] [*path*]

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
disk:	(Optional) Changes the current working directory.
path	(Optional) Directory location.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If a file exists in the directory, the command fails. The **rmdir** command asks you for confirmation before removing the directory. The **rmdir disk:** command prompts you to enter the name of the directory that you are removing.

Examples

This example shows how to remove an existing directory:

```
fwsm(config)# rmdir test
```

Related Commands

cd
copy disk
copy flash
copy startup-config
copy tftp
dir
format
mkdir
more

pwd
rename
show file

route

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

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

Syntax Description

interface_name	Internal or external network interface name.
ip_address	Internal or external network IP address.
netmask	Network mask to apply to *ip_address*.
gateway_ip	IP address of the gateway router (the next-hop address for this route).
metric	(Optional) Number of hops to *gateway_ip*.

Defaults

metric is 1.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

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.

If you are not sure about the number of hops to *gateway_ip*, enter **1**. Your network administrator can supply this information or you can use a **traceroute** command to obtain the number of hops.

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.

```
fwsm/context_name(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

The routing table automatically specifies the IP address of a FWSM interface in the **route** command. Once you enter the IP address for each interface, the FWSM creates a **route** statement entry that is not deleted when you use the **clear route** command.

If the **route** command uses the IP address from one of the FWSM's interfaces 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

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

```
fwsm/context_name(config)# route outside 0 0 209.165.201.1 1
```

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

```
fwsm/context_name(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
fwsm/context_name(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

Related Commands

clear route
show route

route-map

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

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

Syntax Description

map_tag	Text for the route map tag; the text can be up to 58 characters in length.
permit	(Optional) Specifies that if the match criteria is met for this route map, the route is redistributed as controlled by the set actions.
deny	(Optional) Specifies that if the match criteria are met for the route map, the route is not redistributed.
seq_num	(Optional) Route map sequence number; valid values are from 0 to 65535.

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

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: privileged mode

Transparent Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **route-map** command allows you to redistribute routes or to subject packets to policy routing.

The **route-map** global configuration command and the **match** and **set route-map** 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 give 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 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.

Another purpose of route maps is to enable policy routing. Use the **ip policy route-map** command, in addition to the **route-map** command, and the **match** and **set** commands to define the conditions for policy routing packets. The **match** commands specify the conditions under which policy routing occurs. The **set** commands specify the routing actions to perform if the criteria enforced by the **match** commands are met. You might want to specify policy route packets in a way other than the obvious shortest path.

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.

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

This example show how to configure a route map in OSPF routing:

```
fwsm(config)# route-map maptag1 permit 8
fwsm#(config-route-map)# set metric 5
fwsm#(config-route-map)# match metric 5
fwsm#(config-route-map)# set metric-type type-2
fwsm#(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
set metric-type type-2
match metric 5
fwsm#(config-route-map)# exit
fwsm#(config)#
```

Related Commands

clear route-map
match interface (route map submode)
match ip next-hop (route map submode)
match ip route-source (route map submode)
match metric (route map submode)
match route-type (route map submode)
set ip next-hop
set metric
set metric-type
show route-map

router

To configure the router's IP address, use the **router** command. To remove the router ID, use the **no** form of this command.

[**no**] **router** *ip_address*

Syntax Description

ip_address	Router ID in IP address format.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Transparent Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to configure the router's IP address:

```
fwsm(config)# router 122.34 45.10
```

Related Commands

show router

router-id

To configure the fixed router ID for an Open Shortest Path First (OSPF) process, use the **router-id** command. To use the previous OSPF router ID behavior, use the **no** form of this command to reset the OSPF.

[**no**] **router-id** *ip_address*

Syntax Description

ip_address	Router ID in IP address format.

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Transparent Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

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 (DBDs). To prevent this situation, set the **router-id** *ip_address* to a global address.

Examples

This example shows how to configure the fixed router ID for OSPF:

```
fwsm(config)# router-id 123.45.46.10
```

Related Commands

router ospf
show ospf
show routing
show router-id

router ospf

To enable OSPF routing through the FWSM, use the **router ospf** command. To terminate the OSPF routing process specified by its *pid*, use the **no** form of this command.

[**no**] **router ospf** *pid*

Syntax Description

pid	Internally used identification parameter for an OSPF routing process; valid values are from 1 to 65534.

Defaults

OSPF routing is disabled on the FWSM.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF protocol is used instead of the Routing Information Protocol (RIP). Do not attempt to configure the FWSM for both OSPF and RIP at the same time.

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 the submode.

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*.

The **show ospf** command displays the configured **router ospf** subcommands.

You assign the *pid* locally on the firewall. You must assign a unique value for each OSPF routing process.

Once you enter the **route-ospf** command, the command prompt appears as (config-router)#, indicating that you are in the submode.

The **router ospf** command is used with the following OSPF-specific subcommands 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 type 7 default in the NSSA area.

- **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.
- **network**—Defines the interfaces on which OSPF runs and the area ID for those interfaces.
- **redistribute**—Configures the redistribution between OSPF processes according to the parameters specified.
- **router-id**—Creates a fixed router ID.
- **summary-address**—Creates the aggregate addresses for OSPF.
- **timers**—Configures the OSPF process delay timers.

Examples

This example shows how to enter the submode on the outside interface of the FWSM:

```
fwsm(config)# router ospf 5
```

Related Commands

route-map
routing interface
show ip ospf
See also the list of subcommands in the "Usage Guidelines" section.

routing interface

To configure interface-specific Open Shorttest Path First (OSPF) routing parameters, use the **routing interface** command. To remove the routing configuration for the interface specified only, use the **no** form of this command.

[**no**] **routing interface** *interface_name*

Syntax Description

interface_name	Name of the interface to configure.

Defaults

OSPF routing is disabled on the FWSM interfaces.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Usage Guidelines

The **routing interface** *interface_name* command is the main command for all interface-specific OSPF interface mode commands. Enter this command with the name of the FWSM interface (*interface_name*) that you want to configure, and then proceed with interface-specific configuration through the **routing interface** subcommands. You do not need to specify optional arguments in the **no** forms of the **routing interface** subcommands (unless they provide necessary information).

Examples

This example shows how to enter the submode on the outside interface of the FWSM:

```
fwsm(config)# routing interface outside
```

Note In the routing submode, the command prompt appears as "(config-routing)#".

This example shows the configuration for two concurrently running OSPF processes, with the IDs 5 and 12, on the outside interface of the FWSM:

```
fwsm(config)# routing interface
fwsm(config)# show ospf

Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

```
Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

This example shows how to change the retransmit interval to 15 seconds:

```
fwsm(config)# ospf retransmit-interval 15
```

Related Commands

ospf (interface submode)
route-map
router ospf

rpc-server

To create the remote processor call (RPC) services table, use the **rpc-server** command. To remove the RPC services table from the configuration, use the **no** form of this command.

[**no**] **rpc-server** *ifc_name ip_addr mask* **service s***ervice_type* **protocol** [**TCP | UDP**] **port** *port* [*-port*] **timeout** *hh:mm:ss*

no rpc-server active service *service_type* **server** *ip_addr*

Syntax Description

ifc_name	Server interface name.
ip_addr	RPC server IP address.
mask	Network mask.
service	Specifies a service.
service_type	Sets the RPC service program number as specified in the **rpcinfo** command.
protocol tcp *or* **udp**	Specifies the RPC transport protocol.
port *port* [- *port*]	Specifies the RPC protocol port range.
port- *port*	(Optional) Specifies the RPC protocol port range.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the RPC service traffic is closed.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to create an RPC services table:

```
fwsm/context_name(config)# rpc-server inside 30.26.0.23 255.255.0.0 service 2147483647
protocol TCP port 2222 timeout 0:03:00
```

Related Commands

clear rpc-server
show rpc-server

same-security-traffic

To enable same-security level interface communication, use the **same-security-traffic** command. To disable the same-security interfaces, use the **no** form of this command.

[**no**] **same-security-traffic permit inter-interface**

[**no**] **same-security-traffic permit intra-interface**

Syntax Description

permit	Enables same-security level interface communication.
inter-interface	Specifies that communication between two different interfaces with the same security level is being enabled.
intra-interface	Specifies that communication between two hosts in the same interface is enabled.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command with the inter-interface keyword was introduced on the FWSM.
2.3(1)	Support for the Intra-interface keyword was added.

Usage Guidelines

For the intra-interface outside, NAT is not supported. You can configure a static NAT from one interface to another on the same security level.

The intra-interface optioin is not supported in transparent mode.

Examples

This example shows how to enable the same-security interface communication:

```
fwsm/context_name(config)# same-security-traffic permit inter-interface
fwsm/context_name(config)# show same-security-traffic
same-security-traffic permit inter-interface

fwsm/context_name(config)# same-security-traffic permit intra-interface
fwsm/context_name(config)# show same-security-traffic
same-security-traffic permit intra-interface
```

Related Commands clear same-security-traffic
show same-security-traffic

service

To enable system services, use the **service** command. To disable system services, use the **no** form of this command.

[**no**] **service** {**resetinbound** | **resetoutside**}

Syntax Description

resetinbound	Sends a reset to a denied inbound TCP packet.
resetoutside	Sends a reset to a denied TCP packet to the outside interface.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **service** command works with all inbound TCP connections to static interfaces whose access lists or uauth (user authorization) do not allow inbound connections. One use is for resetting identity request (IDENT) connections. If an inbound TCP connection is attempted and denied, you can use the **service resetinbound** command to return an RST (reset flag in the TCP header) to the source. Without the keyword, the FWSM drops the packet without returning an RST.

The FWSM sends a TCP RST to the host connecting inbound and stops the incoming IDENT process so that outbound e-mail can be transmitted without having to wait for IDENT to time out. The FWSM sends a syslog message stating that the incoming connection was denied. Without entering the **service resetinbound** command, the FWSM drops packets that are denied and generates a syslog message stating that the SYN was denied. However, outside hosts keep retransmitting the SYN until the IDENT times out.

When an IDENT connection times out, the connections slow down. Perform a trace to determine that IDENT is causing the delay and then enter the **service** command.

Use the **service resetinbound** command to handle an IDENT connection through the FWSM. These methods for handling IDENT connections are ranked from most secure to the least secure:

1. Use the **service resetinbound** command.
2. Use the **established** command with the **permitto tcp 113** keyword.
3. Enter the **static** and **access-list** commands to open TCP port 113.

When using the **aaa** command, if the first attempt at authorization fails and a second attempt causes a timeout, use the **service resetinbound** command to reset the client that failed the authorization so that it will not retransmit any connections. An example authorization timeout message in Telnet is as follows:

```
Unable to connect to remote host: Connection timed out
```

If you use the **resetoutside** command, the FWSM actively resets denied TCP packets that terminate at the FWSMs least-secure interface. By default, these packets are silently discarded. We recommend that you use the **resetoutside** keyword with dynamic or static interface Port Address Translation (PAT). The static interface PAT is available with FWSM version 6.0 and higher. This keyword allows the FWSM to terminate the IDENT from an external SMTP or FTP server. Actively resetting these connections avoids the 30-second timeout delay.

To remove the **service** commands from the configuration, use the **clear service** command.

Examples

This example shows how to enable system services:

```
fwsm/context_name(config)# service resetinbound
```

Related Commands

clear service
show service

set (route map submode)

To specify the values in the destination routing protocol for a route map, use the **set** command in the route-map submode. To delete an entry, use the **no** form of this command.

[**no**] **set metric** [**+** | **-**] *metric_value*

[**no**] set **metric-type** {**type-1** | **type-2** | **internal** | **external**}

Syntax Description

metric	Specifies metric values.
+ or **-**	(Optional) Specifies positive or negative metric values.
metric_value	Metric value; valid values are from 0 to 2147483647.
metric-type	Specifies the type of OSPF metric routes.
type-1	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
type-2	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
internal	Specifies routes that are internal to a specified autonomous system.
external	Specifies the OSPF metric routes that are external to a specified autonomous system.
ip-address	IP address of the next hop to which to output packets.
ip-address	(Optional) IP address of the secondary next hop.

Defaults

Default metric value; valid values are from -2147483647 to 2147483647.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to send packets passed by a match clause of a route map:

```
fwsm(config-route-map)# set metric + 56789
```

Related Commands

match (route map submode)
route-map
set metric (route map submode)

set metric-type (route map submode)
show route-map
show set

set metric (route map submode)

To set the metric value for a routing protocol, use the **set metric** subcommand. To return to the default metric value, use the **no** form of this command.

set metric [**+** | **–**] *metric_value*

[**no**] **set metric** *value*

Syntax Description

+ or **–**	Specifies positive or negative values.
metric_value	Metric value; valid values are from 0 to 2147483647.
value	Default metric value; valid values are from –2147483647 to 2147483647.

Defaults

–2147483647 to 2147483647.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **no set metric** *value* subcommand allows you to return to the default metric value. In this context, the *value* is an integer from –2147483647 to 2147483647.

Examples

This example shows how to configure a route map for OSPF routing:

```
fwsm(config)# route-map maptag1 permit 8
fwsm(config-route-map)# set metric 5
fwsm(config-route-map)# match metric 5
fwsm(config-route-map)# set metric-type type-2
fwsm(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
fwsm(config-route-map)# exit
fwsm(config)#
```

Related Commands

match (route map submode)
route-map
set metric-type (route map submode)
show route-map
show set

set metric-type (route map submode)

To specify the type of OSPF metric routes, use the **set metric-type** subcommand. To return to the default setting, use the **no** form of this command.

set metric-type {**type-1 | type-2 | internal | external**}

no set metric-type

Syntax Description

type-1	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
type-2	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
internal	Specifies the routes that are internal to a specified autonomous system.
external	Specifies the OSPF metric routes that are external to a specified autonomous system.

Defaults

type-2

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example show how to configure a route map for OSPF routing:

```
fwsm(config)# route-map maptag1 permit 8
fwsm(config-route-map)# set metric 5
fwsm(config-route-map)# match metric 5
fwsm(config-route-map)# set metric-type type-2
fwsm(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
fwsm(config-route-map)# exit
fwsm(config)#
```

Related Commands

route-map
set metric (route map submode)
set metric-type (route map submode)
show route-map
show set

setup

To preconfigure the FWSM through interactive prompts, use the **setup** command.

setup

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The FWSM requires some preconfiguration before the PDM can connect to it. The setup dialog automatically appears at boot time if there is no configuration in the Flash partition. Once you enter the **setup** command, you are asked for the setup information in Table 2-14.

Table 2-14 FWSM Setup Information

Prompt	Description
`Firewall Mode`	Valid values are routed or transparent, or variations of these values. For example, r or t for routed or transparent are valid values.
`Enable password:`	Specify an enable password for this FWSM. (The password must have at least three characters.)
`Inside IP address:`	Network interface IP address of the FWSM.
`Inside network mask:`	Network mask that applies to the inside IP address must be a valid mask such as 255.0.0.0, 255.255.0.0, or 255.255.x.x. Use 0.0.0.0 to specify a default route. The 0.0.0.0 netmask can be abbreviated as 0.
`Host name:`	Host name that you want to display in the FWSM command line prompt.
`Domain name:`	DNS domain name of the network on which the FWSM runs.

Table 2-14 FWSM Setup Information (continued)

IP address of host running Device Manager:	IP address on which the PDM connects to the FWSM.
Use this configuration and write to flash?	Stores the new configuration to the Flash partition. If the answer is **yes**, the inside interface is enabled and the requested configuration is written to the Flash partition. If the user answers anything else, the setup dialog repeats the values that are already entered as the defaults for the questions.

You must configure an inside interface before this command can be used. If you do not configure an insie interface, the *No inside interface. Can not continue.* error is displayed.

The host and domain names are used to generate the default certificate for the Secure Socket Layer (SSL) connection. The interface type is determined by the hardware.

Examples

This example shows how to complete the **setup** command prompts. This example assumes that VLAN 100 has been configured on the switch as a firewall VLAN. This example shows an inside interface being defined followed by the setup command with the FWSM being placed in routed mode.

```
FWSM(config)# setup
Pre-configure FWSM Firewall now through interactive prompts [yes]? y
Firewall Mode [Routed]:
No inside interface.  Can not continue.
FWSM(config)# nameif vlan100 inside 100
FWSM(config)# setup
Pre-configure FWSM Firewall now through interactive prompts [yes]? y
Firewall Mode [Routed]:
Enable password [<use current password>]: ciscofwsm
Inside IP address [127.0.0.1]: 192.168.1.1
Inside network mask [255.255.255.255]: 255.255.255.0
Host name [FWSM]: accounting-fwsm
Domain name: example.com
IP address of host running FWSM Device Manager: 192.168.1.2

The following configuration will be used:
Enable password: ciscofwsm
Clock (UTC): 11:37:36 Mar 8 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: accounting-fwsm
Domain name: example.com
IP address of host running FWSM Device Manager: 192.168.1.2

Use this configuration and write to flash? y
Building configuration...
Cryptochecksum: 2e02e1d2 019721a8 981ec7f8 19bbc74b
[OK]
accounting-fwsm(config)# Access Rules Download Complete: Memory Utilization: < 1%
```

Related Commands

pdm

show

To display the information about the commands, use the **show** command.

show *command_keywords* [|{**include** | **exclude** | **begin** | **grep** [**-v**]} *regexp*]

show ?

Syntax Description

command_keywords	Argument or list of arguments that specifies the information to display.
|	UNIX pipe symbol, "|".
include	(Optional) Includes all output lines that match the specified regular expression.
exclude	(Optional) Excludes all output lines that match the specified regular expression.
begin	(Optional) Displays all output lines starting from the line that matches the specified regular expression.
grep	(Optional) Displays all output lines that match the specified regular expression. **grep** is equivalent to **include**, and **grep -v** is equivalent to **exclude**.
-v	(Optional) When used withthe **grep** keyword, the **-v** option is equivilent to an exclude statement.
regexp	(Optional) Cisco IOS-style regular expression.

Defaults

See each command for the default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show** *command_keywords* [|{**include | exclude | begin | grep**} *regexp*] command runs the **show** command keyword specified. Only the first "|" is a pipe character in this syntax. This character represents piping output to the filter. When "|" is present, a filtering keyword and a regular expression must also be present.

The CLI syntax and semantics of the **show** output filtering options are the same as in Cisco IOS software and are available through the console, Telnet, or SSH sessions.

Most commands have a **show** command form where the command name is used as a **show** keyword. For example, the **global** command has an associated **show global** command.

The **show ?** command displays a list of all commands that are available on the FWSM.

Do not enclose the *regexp* argument in quotes or double quotes. Additionally, trailing white spaces (between keywords) are taken as part of the regular expression.

Examples

This example shows how to use a **show** command output filter keyword, where the "|" is the UNIX pipe symbol:

```
fwsm(config)# show config | grep access-list
access-list 101 permit tcp any host 10.1.1.3 eq www
access-list 101 permit tcp any host 10.1.1.3 eq smtp
```

This example shows sample output from the **show ?** command:

```
fwsm(config)# show ?

At the end of show <command>, use the pipe character '|' followed by:
begin|include|exclude|grep [-v] <regular_exp>, to filter show output.

aaa             Enable, disable, or view TACACS+, RADIUS or LOCAL
                user authentication, authorization and accounting
aaa-server      Define AAA Server group
access-group    Bind an access-list to an interface to filter inbound traffic
access-list     Add an access list
activation-key  Modify activation-key.
age             This command is deprecated. See ipsec, isakmp, map, ca commands
alias           Administer overlapping addresses with dual NAT.
apply           Apply outbound lists to source or destination IP addresses
arp             Change or view arp table, set arp timeout value and view status
auth-prompt     Customize authentication challenge, reject or acceptance prompt
auto-update     Configure auto update support
banner          Configure login/session banners
blocks          Show system buffer utilization
ca              CEP (Certificate Enrollment Protocol)
                Create and enroll RSA key pairs into a PKI (Public Key Infrastr.
capture         Capture inbound and outbound packets on one or more interfaces
checksum        View configuration information cryptochecksum
chunkstat       Display chunk stats
clock           Show and set the date and time of FWSM
configure       Configure from terminal, floppy, memory, network, or
                factory-default.  The configuration will be merged with the
                active configuration except for factory-default in which case
                the active configuration is cleared first.
conn            Display connection information
console         Set idle timeout for the serial console of the FWSM
cpu             Display cpu usage
Crashinfo       Read, write and configure crash write to flash.
crypto          Configure IPsec, IKE, and CA
ctiqbe          Show the current data stored for each CTIQBE session.
curpriv         Display current privilege level
debug           Debug packets or ICMP tracings through the FWSM Firewall.
dhcpd           Configure DHCP Server
dhcprelay       Configure DHCP relay agent
domain-name     Change domain name
dynamic-map     Specify a dynamic crypto map template
eeprom          show or reprogram the 525 onboard i82559 devices
enable          Configure enable passwords
established     Allow inbound connections based on established connections
failover        Enable/disable FWSM failover feature to a standby FWSM
filter          Enable, disable, or view URL, FTP, HTTPS, Java, and ActiveX filg
fips-mode       Enable or disable FIPS mode
fixup           Add or delete FWSM service and feature defaults
```

```
flashfs          Show, destroy, or preserve filesystem information
fragment         Configure the IP fragment database
global           Specify, delete or view global address pools,
                 or designate a PAT(Port Address Translated) address
h225             Show the current h225 data stored for each connection.
h245             List the h245 connections.
h323-ras         Show the current h323 ras data stored for each connection.
history          Display the session command history
http             Configure HTTP server
icmp             Configure access for ICMP traffic that terminates at an interfae
interface        Set network interface paremeters and configure VLANs
igmp             Clear or display IGMP groups
ip               Set the ip address and mask for an interface
                 Define a local address pool
                 Configure Unicast RPF on an interface
                 Configure the Intrusion Detection System
ipsec            Configure IPSec policy
isakmp           Configure ISAKMP policy
local-host       Display or clear the local host network information
logging          Enable logging facility
mac-list         Add a list of mac addresses using first match search
map              Configure IPsec crypto map
memory           System memory utilization
mgcp             Configure the Media Gateway Control Protocol fixup
mroute           Configure a multicast route
mtu              Specify MTU(Maximum Transmission Unit) for an interface
multicast        Configure multicast on an interface
name             Associate a name with an IP address
nameif           Assign a name to an interface
names            Enable, disable or display IP address to name conversion
nat              Associate a network with a pool of global IP addresses
ntp              Configure Network Time Protocol
object-group     Create an object group for use in 'access-list', etc
ospf             Show OSPF information or clear ospf items.
outbound         Create an outbound access list
pager            Control page length for pagination
passwd           Change Telnet console access password
pdm              Configure FWSMDevice Manager
prefix-list      Configure a prefix-list
privilege        Configure/Display privilege levels for commands
processes        Display processes
rip              Broadcast default route or passive RIP
route            Enter a static route for an interface
route-map        Create a route-map.
router           Create/configure OSPF routing process
routing          Configure interface specific unicast routing parameters.
running-config   Display the current running configuration
service          Enable system services
session          Access an internal AccessPro router console
shun             Manages the filtering of packets from undesired hosts
sip              Show the current data stored for each SIP session.
skinny           Show the current data stored for each Skinny session.
snmp-server      Provide SNMP and event information
ssh              Add SSH access to FWSM console, set idle timeout, display
                 list of active SSH sessions & terminate a SSH session
startup-config   Display the startup configuration
static           Configure one-to-one address translation rule
tcpstat          Display status of tcp stack and tcp connections
tech-support     Tech support
telnet           Add telnet access to FWSM console and set idle timeout
terminal         Set terminal line parameters
tftp-server      Specify default TFTP server address and directory
timeout          Set the maximum idle times
traffic          Counters for traffic statistics
```

```
uauth           Display or clear current user authorization information
url-cache       Enable URL caching
url-block       Enable URL pending block buffer and long URL support
url-server      Specify a URL filter server
username        Configure user authentication local database
version         Display FWSM system software version
virtual         Set address for authentication virtual servers
vpdn            Configure VPDN (PPTP, L2TP, PPPoE) Policy
vpnclient       Configure Easy VPN Remote
vpngroup        Configure group settings for Cisco VPN Clients and
                Cisco Easy VPN Remote products
who             Show active administration sessions on FWSM
xlate           Display current translation and connection slot information
```

show aaa

To display the local, TACACS+, or RADIUS user accounting, use the **show aaa** command.

show aaa

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support a second LOCAL method for AAA configurations.

Examples

This example shows how to display the local, TACACS+, or RADIUS user accounting:

```
fwsm/context_name(config)# show aaa
```

Related Commands

aaa accounting match
aaa authentication
aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

show aaa proxy-limit

To display the number of concurrent proxy connections that are allowed per user, use the **show aaa proxy-limit** command.

show aaa proxy-limit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show aaa proxy-limit** command allows you to display the number of outstanding authentication requests that are allowed or indicates that the proxy limit is disabled if you disabled it.

Examples

This example shows how to display the number of concurrent proxy connections that are allowed per server:

```
fwsm/context_name(config)# show aaa proxy-limit
```

Related Commands

aaa accounting match
aaa authentication
aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

show aaa-server

To display the AAA server configuration information, use the **show aaa-server** command.

show aaa-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support a second LOCAL method for AAA configurations.

Examples

This example shows how to display the AAA server configuration information:

```
fwsm/context_name(config)# show aaa-server
```

Related Commands

aaa accounting match
aaa authentication
aaa authorization
auth-prompt
password/passwd
service
ssh
telnet
virtual

show access-group

To bind an access list to an interface, use the **show access-group** command.

show access-group

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to bind an access list to an interface:

```
FWSM# show access-group
access-group outside_in in interface inside
access-group 100 out interface inside
```

Related Commands

access-group

show access-list

To display the access list entries, use the **show access-list** command.

show access-list [*id*]

Syntax Description

id	(Optional) Access list.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how the FWSM displays access list entries.

```
fwsm(config)# show access-list ac
access-list ac; 2 elements
access-list ac permit ip any any (hitcnt=0)
access-list ac permit tcp any any (hitcnt=0)
```

Related Commands

access-list extended
clear access-list
show access-list mode

show access-list mode

To display the compilation mode for the system, use the **show access-list mode** command.

show access-list mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the access list compilation mode for the FWSM:

```
fwsm(config)# show access-list mode
access-list mode manual-commit
```

Related Commands

access-list extended
access-list mode
clear access-list
show access-list

show activation-key

To display the commands in the configuration for features that are enabled by your activation key, including the number of contexts allowed, use the **show activation-key** command.

show activation-key

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show activation-key** command output indicates the status of the activation key as follows:

- If the activation key in the FWSM Flash partition is the same as the activation key running on the FWSM, then the **show activation-key** output reads as follows:

```
The flash activation key is the SAME as the running key.
```

- If the activation key in the FWSM Flash partition is different from the activation key running on the FWSM, then the **show activation-key** output reads as follows:

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- If the FWSM Flash partition software image version is not the same as the running FWSM software image, then the **show activation-key** output reads as follows:

```
The flash image is DIFFERENT from the running image.
The two images must be the same in order to examine the flash activation key.
```

- If you downgrade your activation key, the display shows that the running key (the old key) differs from the key that is stored in the Flash (the new key). When you restart, the FWSM uses the new key.
- If you upgrade your key to enable extra features, the new key starts running immediately without a restart.

Examples

This example shows how to display the commands in the configuration for features that are enabled by your activation key:

```
fwsm(config)# show activation-key
Running Activation Key: 0x00000000 0x00000000 0x00000000 0x00000000
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 100 (per security context)
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Throughput:         Unlimited
ISAKMP peers:       Unlimited
Security Contexts:  2
This machine has an Unrestricted (UR) license.
The flash activation key is the SAME as the running key.
fwsm(config)#
```

Related Commands

activation-key
clear

show admin-context

To display which context is designated as the administration context, use the **show admin-context** command.

show admin-context

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the designated administration context:

```
fwsm(config)# show admin-context
Admin: admin disk:/admin.cfg
```

Related Commands

admin-context

show alias

To display the overlapping addresses with dual NAT commands in the configuration, use the **show alias** command.

show alias

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display alias information:

```
fwsm/context_name(config)# show alias
fwsm/context_name(config)#
```

Related Commands

alias

show area

To display the **area** commands in the configuration, use the **show area** command.

show area

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display area command configuration information:

```
fwsm/context_name(config)# show area
```

Related Commands

area

show arp

To list the entries in the ARP table, use the **show arp** command.

show arp [**timeout** | **statistics**]

Syntax Description

timeout	(Optional) Specifies ARP timeout information.
statistics	(Optional) Specifies ARP statistics.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line and context command line

Command Mode: configuration mode and privileged mode

Firewall Mode: routed firewall mode and transparent mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to list the entries in the ARP table:

```
fwsm(config)# show arp statistics
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

Related Commands

arp
arp-inspection

show auth-prompt

To display the current AAA challenge text, use the **show auth-prompt** command.

show auth-prompt

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the AAA challenge text:

```
fwsm/context_name(config)# show auth-prompt
```

Related Commands

auth-prompt

show banner

To display the specified banner and all the lines that are configured for it, use the **show banner** command.

show banner [{**exec** | **login** | **motd**}]

Syntax Description

exec	(Optional) Displays the banner before the enable prompt.
login	(Optional) Displays the banner seen before the password login prompt when accessing the FWSM using Telnet.
motd	(Optional) Displays the message-of-the-day banner.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show banner** {**motd** | **exec** | **login**} command allows you to display the specified banner keyword and all the lines that are configured for it. If you do not specify a banner keyword, then all the banners are displayed.

Examples

This example shows how to display the message-of-the-day (motd) banner:

```
fwsm/context_name(config)# show banner motd
```

Related Commands

banner
clear banner

show blocks

To display the blocks in the preallocated system buffer, use the **show blocks** command.

show blocks [**address** *hex-address* | **all** | **assigned** | **free** | **old** | **pool** *block-size* | **queue history** [**detail**] [**dump** | **header** | **packet**]]

Syntax Description

address *hex-address*	(Optional) Specifies the block address.
all	(Optional) Specifies all blocks.
assigned	(Optional) Specifies the assigned blocks.
free	(Optional) Specifies the free blocks.
old	(Optional) Specifies the old blocks.
pool *block-size*	(Optional) Specifies a block pool and size.
queue history	(Optional) Specifies the queue history.
detail	(Optional) Specifies the block details.
dump	(Optional) Specifes a block dump.
header	(Optional) Specifies a header.
packet	(Optional) Specifies a packet.

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was updated on the FWSM.

Usage Guidelines

The **show blocks** command allows you to determine whether the FWSM is being overloaded similarly to the **show cpu** command. The **show blocks** command allows you to display preallocated system buffer utilization.

In the **show blocks** command listing, the SIZE column displays the block type. The MAX column is the maximum number of allocated blocks. The LOW column is the fewest blocks that are available since the last reboot. The CNT column is the current number of available blocks. A zero in the LOW column indicates a previous event where memory is full. A zero in the CNT column means memory is full now. A full memory condition is not a problem as long as traffic is moving through the FWSM.

You can use the **show conn** command to see if traffic is moving. If traffic is not moving and the memory is full, there may be a problem.

You can also display the information from the **show blocks** command using SNMP.

Packet-Processing Blocks (1550 and 16384 Bytes)

When a packet enters an FWSM's interface, it is placed on the input interface queue, passed up to the operating system, and placed in a block. For Ethernet packets, the 1550-byte blocks are used; if the packet comes in on a 66-MHz Gigabit Ethernet card, the 16384-byte blocks are used. The FWSM determines whether the packet should be permitted or denied based on the adaptive security algorithm (ASA) and processes the packet through to the output queue on the outbound interface. If the FWSM is having trouble keeping up with the traffic load, the number of available 1550-byte blocks (or 16384-byte blocks for 66-MHz GE) will hover close to 0 (as shown in the CNT column of the command output). When the CNT column is zero, the FWSM attempts to allocate more blocks, up to a maximum of 8192. If no more blocks are available, the FWSM drops the packet.

Failover and syslog Blocks (256 Bytes)

The 256-byte blocks are mainly used for stateful failover messages. The active FWSM generates and sends packets to the standby FWSM to update the translation and connection table. In bursty traffic, where high rates of connections are created or torn down, the number of available 256-byte blocks may drop to 0. This situation indicates that one or more connections were not updated to the standby FWSM. The stateful failover protocol will catch the missing xlate or connection the next time. If the CNT column for 256-byte blocks stays at or near 0 for extended periods of time, then the FWSM is having trouble keeping the translation and connection tables synchronized because of the number of connections per second that the FWSM is processing. If this situation happens consistently, you might upgrade the FWSM to a faster model.

The syslog messages that are sent out from the FWSM also use the 256-byte blocks, but they are generally not released in such quantity to cause a depletion of the 256-byte block pool. If the CNT column shows that the number of 256-byte blocks is near 0, ensure that you are not logging at Debugging (level 7) to the syslog server. This is indicated by the logging trap line in the FWSM configuration. We recommend that you set logging at Notification (level 5) or lower, unless you require additional information for debugging purposes.

Table 2-15 describes the columns in the **show blocks** display.

Table 2-15 Display Column Description

Column	Description
SIZE	Size, in bytes, of the block pool.
MAX	Maximum number of blocks available for the specified byte block pool. The maximum number of blocks are carved out of memory at bootup. Typically, the maximum number of blocks does not change. The exception is for the 256- and 1550-byte blocks, where the FWSM can dynamically create more when needed, up to a maximum of 8192.
LOW	Low-water mark. This number indicates the lowest number of this size blocks available since the FWSM was powered up, or since the last clearing of the blocks (with the **clear blocks** command).
CNT	Current number of blocks available for that specific size block pool.

Table 2-16 describes the rows in the **show blocks** display.

Table 2-16 Display Row Description

Size	Description
4	Duplicates existing blocks in DNS, Internet Security Association and Key Management Protocol (ISAKMP), URL filtering, uauth, TFTP, and TCP modules.
80	Used in TCP intercept to generate acknowledgment (ACK) packets and for failover hello messages.
256	Used for stateful failover updates, syslogging, and other TCP functions.
1550	Used to store Ethernet packets for processing through the FWSM.
16384	Only used for the 64-bit, 66-MHz Gigabit Ethernet cards (i82543).
2048	Control or guided frames used by the network processors (NP) for control updates.

Examples

This example show how to display preallocated system buffer memory blocks:

```
fwsm(config)# show blocks
  SIZE     MAX     LOW     CNT
     4    1600    1600    1600
    80     100      97      97
   256      80      79      79
  1550     788     402     404
 65536       8       8       8
  2048    1000     994    1000
```

Related Commands

clear blocks

show ca

To display the certificate authorization information, use the **show ca** command.

show ca {**certificate** | **crl** | **configure** | **identity** | **mypubkey rsa** | **subject-name** | **verifycertdn**}

Syntax Description

certificate	Displays the current status of requested certificates and relevant information of received certificates, such as CA and RA certificates.
crl	Displays whether there is a CRL in RAM, and where and when the CRL is downloaded.
configure	Displays the current communication parameter settings that are stored in the FWSM RAM.
identity	Displays the current CA settings that are stored in RAM.
mypubkey rsa	Displays the FWSM's public keys in a DER/BER encoded PKCS#1 representation.
subject-name	Displays the subject Distinguished Name (DN).
verifycertdn	Displays the certificate's Distinguished Name (DN).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the current status of requested certificates. The CA certificate stems from a Microsoft CA server that was previously generated for this FWSM.

```
fwsm(config)# show ca certificate

RA Signature Certificate
  Status:Available
  Certificate Serial Number:6106e08a000000000005
  Key Usage:Signature
    CN = SCEP
     OU = VSEC
     O = Cisco
     L = San Jose
     ST = CA
     C = US
     EA =<16> username@example.com
```

```
  Validity Date:
    start date:17:17:09 Jul 11 2000

    end   date:17:27:09 Jul 11 2001

Certificate
  Status:Available
  Certificate Serial Number:1f80655400000000000a
  Key Usage:General Purpose
  Subject Name
    Name:firewall.example.com
  Validity Date:
    start date:20:06:23 Jul 17 2000

    end   date:20:16:23 Jul 17 2001

CA Certificate
  Status:Available
  Certificate Serial Number:25b81813efe58fb34726eec44ae82365
  Key Usage:Signature
    CN = MSCA
     OU = Cisco
     O = VSEC
     L = San Jose
     ST = CA
     C = US
     EA =<16> username@example.com
  Validity Date:
    start date:17:07:34 Jul 11 2000
RA KeyEncipher Certificate
  Status:Available
  Certificate Serial Number:6106e24c000000000006
  Key Usage:Encryption
    CN = SCEP
     OU = VSEC
     O = Cisco
     L = San Jose
     ST = CA
     C = US
     EA =<16> username@example.com
  Validity Date:
    start date:17:17:10 Jul 11 2000

    end   date:17:27:10 Jul 11 01
```

Table 2-17 describes strings within the **show ca certificate** command sample output.

Table 2-17 Command Sample Output

Sample Output String	Description
CN	Common name
C	Country
EA	E-mail address
L	Locality
ST	State or province
O	Organization name

Table 2-17 Command Sample Output (continued)

Sample Output String	Description
OU	Organizational module name
DC	Domain component

This example shows how to display certificate information. See Table 2-17 for descriptions of the strings within the following sample output.

```
fwsm(config)# show ca crl

CRL:
    CRL Issuer Name:
        CN = MSCA, OU = Cisco, O = VSEC, L = San Jose, ST = CA, C = US, EA
=<16> username@example.com
    LastUpdate:17:07:40 Jul 11 2000

    NextUpdate:05:27:40 Jul 19 2000
```

This example shows how to display information about the RSA keys. Special-usage RSA keys were previously generated for this FWSM using the **ca generate rsa** command.

```
fwsm(config)# show ca mypubkey rsa

% Key pair was generated at: 15:34:55 Aug 05 1999

Key name: firewall.example.com
 Usage: Signature Key
 Key Data:
  305c300d 06092a86 4886f70d 01010105 00034b00 30480241 00c31f4a ad32f60d
  6e7ed9a2 32883ca9 319a4b30 e7470888 87732e83 c909fb17 fb5cae70 3de738cf
  6e2fd12c 5b3ffa98 8c5adc59 1ec84d78 90bdb53f 2218cfe7 3f020301 0001
% Key pair was generated at: 15:34:55 Aug 05 1999

Key name: firewall.example.com
 Usage: Encryption Key
 Key Data:
  305c300d 06092a86 4886f70d 01010105 00034b00 30480241 00d8a6ac cc64e57a
  48dfb2c1 234661c7 76380bd5 72ae62f7 1706bdab 0eedd0b5 2e5feef0 76319d98
  908f50b4 85a291de 247b6711 59b30026 453bfa3c 45234991 5d020301 0001
```

This example shows how to display a certificate with a CRL string. See Table 2-17 for descriptions of the strings within the following sample output.

```
fwsm(config)# show ca crl

CRL:
    CRL Issuer Name:
        CN = MSCA, OU = Cisco, O = VSEC, L = San Jose, ST = CA, C = US, EA
=<16> username@example.com
    LastUpdate:17:07:40 Jul 11 2000

    NextUpdate:05:27:40 Jul 19 2000
```

Related Commands **ca authenticate**

show capture

To display the capture configuration when no options are specified, use the **show capture** command.

show capture [[**context-name/**] [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**detail**] [**dump**]]

Syntax Description

context-name/	(Optional) Context name.
capture_name	(Optional) Name of the packet capture.
access-list *access_list_name*	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
count *number*	(Optional) Displays the packet count.
detail	(Optional) Displays additional protocol information for each packet.
dump	(Optional) Displays a hexadecimal dump of the packets that are transported over the data link transport.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If you specify the *capture_name*, then the capture buffer contents for that capture are displayed.

The **dump** keyword does not display MAC information in the hexadecimal dump.

The decoded output of the packets depend on the protocol of the packet. In Table 2-18, the bracketed output is displayed when you specify the **detail** keyword.

Table 2-18 Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]

Table 2-18 Packet Capture Output Formats (continued)

Packet Type	Capture Output Format
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/Other	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
Other	*HH:MM:SS.ms ether-hdr*: *hex-dump*

Examples

This example shows how to display the capture configuration:

```
fwsm(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

This example shows how to display the packets that are captured by an ARP capture:

```
fwsm(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

Related Commands

capture
clear capture

show checksum

To display the configuration checksum, use the **show checksum** command.

show checksum

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show checksum** command allows you to display four groups of hexadecimal numbers that act as a digital summary of the configuration contents. This same information is stored with the configuration when you store the configuration in the Flash partition. By using the **show config** command, viewing the checksum at the end of the configuration listing, and using the **show checksum** command, you can compare the numbers to see if the configuration has changed. The FWSM tests the checksum to determine if a configuration has not been corrupted.

If a dot (".") appears before the checksum in the **show config** or **show checksum** command output, the output indicates a normal configuration load or write mode indicator (when loading from or writing to the FWSM Flash partition). The "." shows that the FWSM is preoccupied with the operation but is not "hung up." This message is similar to a "system processing, please wait" message.

Examples

This example shows how to display the configuration or the checksum:

```
fwsm(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

To display the chunk statistics, use the **show chunkstat** command.

show chunkstat

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the chunk statistics:

```
fwsm(config)# show chunkstat
Chunk statistics: created 1, destroyed: 0,sibs created: 0, sibs trimmed: 0
Dump of chunk at 0cc835e4, name "Radix trie mask chunks", data start @ 0cc845dc,
 end @ 0cc8845c
 flink: 013ef300, blink: 013ef300
 next: 00000000, next_sibling: 00000000, prev_sibling: 00000000
 flags 00000001
 maximum chunk elt's: 1000, elt size: 16, index first free 997
 # chunks in use: 3, HWM of total used: 3, alignment: 0

Chunk statistics: created 1, destroyed: 0,sibs created: 0, sibs trimmed: 0
Dump of chunk at 0cbd77ec, name "IP subnet NDB entry", data start @ 0cbd8014, en
d @ 0cc66954
 flink: 00000000, blink: 00ed81c8
 next: 00000000, next_sibling: 00000000, prev_sibling: 00000000
 flags 00000009
 maximum chunk elt's: 500, elt size: 1156, index first free 500
 # chunks in use: 0, HWM of total used: 0, alignment: 0
```

show class

To display the class configuration, use the **show class** command.

show class

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: Multiple

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display class configuration information:

```
fwsm(config)# show class
Class Name           Members     ID   Flags
default                All        1    0001
fwsm(config)#
```

Related Commands

class
clear

show clock

To display the FWSM clock for use with the FWSM Syslog Server (PFSS) and the Public Key Infrastructure (PKI) protocol, use the **show clock** command.

show clock

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(2)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the FWSM clock for use with the PFSS and PKI protocols:

```
fwsm/context_name(config)# show clock
08:46:48    [0] Jul 16 2003
```

show compatible rfc1583

To display the method that is used to calculate the summary route costs per RFC 1583, use the **show compatible rfc1583** command.

show compatible rfc1583

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- OSPF routing is disabled on the FWSM.
- OSPF routing through the FWSM is compatible with RFC 1583.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display calculation methods for summary route costs per RFC 1583:

```
fwsm/context_name(config)# show compatible rfc1583
```

Related Commands

compatible rfc1583

show configure

To display the startup configuration of the FWSM, use the **show configure** command.

show configure

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show configure** and **show startup-config** commands allow you to display the startup configuration of the FWSM. The **write terminal** and **show running-config** commands allow you to display the configuration that is currently running on the FWSM.

Examples

This example shows how to display the startup configuration of the FWSM:

```
fwsm/context_name(config)# show configure
: Saved
: Written by enable_15 at 16:17:31 Jun 26 2003

fwsm Version 2.2(0)141
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname sw8fx1
ftp mode passive
names
access-list deny-flow-max 4096
access-list alert-interval 300
no pager
logging history debugging
class default
  limit-resource All 0
!
admin-context admin

context admin
  logical-interface vlan300
  config-url disk:admin.cfg
```

```
!
context my_context
  logical-interface vlan300
  config-url disk:my_context.cfg
!
context my_context
  logical-interface vlan300
  config-url disk:my_context.cfg
!
failover
failover lan unit secondary
failover lan interface failover vlan 500
failover polltime unit 15
failover polltime interface 15
failover interface-policy 50 percent
failover interface ip failover 192.168.1.1 255.255.255.0 standby 192.168.1.2
no pdm history enable
arp timeout 14400
!
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:01:00 rpc 0:10:00 h
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:00:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
floodguard enable
no sysopt route dnat
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:03266426306f5ed3d9eb48b859a7263c
```

Related Commands

clear configure
configure

show conn

To display the connections used and those that are available, use the **show conn** command.

show conn [**count**] | [**protocol** {**TCP** | **UDP** | **icmp**}] [{**foreign** | **local**} *ip* [*-ip2*]] [**netmask** *mask*] [{**lport** | **fport**} *port1* [*-port2*]]

show conn [**state** *up* [,*finin*][,*finout*][,*http_get*][,*smtp_data*][,*data_in*][,*data_out*][,...]]

show conn detail

Syntax Description

count	(Optional) Displays only the number of used connections.
protocol TCP	(Optional) Displays the active TCP connections; see the "Usage Guidelines" section for additional information.
protocol UDP	(Optional) Displays the active UDP connections; see the "Usage Guidelines" section for additional information.
protocol icmp	(Optional) Displays the active ICMP connections; see the "Usage Guidelines" section for additional information.
foreign *ip* **-***ip2*	(Optional) Displays the active connections by the foreign IP address.
local *ip* **-***ip2*	(Optional) Displays the active connections by the local IP address.
netmask *mask*	(Optional) Displays the netmask for the foreign IP address or by the local IP address.
lport *port1* **-***port2*	(Optional) Displays the local active connections by port; see the "Usage Guidelines" section for additional information.
fport *port1* **-***port2*	(Optional) Displays the foreign active connections by port; see the "Usage Guidelines" section for additional information.
state	(Optional) Displays the active connections by their current state; see the "Usage Guidelines" section for additional information.
up	(Optional) Active connections.
,*finin*	(Optional) Foreign connection state in.
,*finout*	(Optional) Foreign connection state out.
,*http_get*	(Optional) HTTP connection state.
smtp_data	(Optional) SMTP connection state.
,*data_in*	(Optional) Data connection state.
,*data_out*	(Optional) Data connection state out.
,...	(Optional) Other connections.
detail	Displays the connection details.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show conn** command allows you to display the number of, and information about, active TCP connections. When specifying multiple **show conn state** keywords, use commas without spaces to list as follows:

```
fwsm(config)# show conn state up,rpc,h323,sip
```

If you insert spaces, the FWSM does not recognize the command.

You can also display the connection count information from the **show conn** command using SNMP.

The accuracy of the displayed count may vary depending on the traffic volume and the type of traffic that is passing through the FWSM.

See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names.

When you enter the **show conn** command, the following active connections are displayed by their current state (listed in bold print):

- Up (**up**)
- Inbound connection (**conn_inbound**)
- Computer Telephony Interface Quick Buffer Encoding (CTIQBE) connection (**ctiqbe**)
- Inbound data (**data_in**)
- Outbound data (**data_out**)
- Dump clean up connection (**dump**)
- FIN inbound (**finin**)
- FIN outbound (**finout**)
- H.225 connection (**h225**)
- H.323 connection (**h323**)
- HTTP get (**http_get**)
- Media Gateway Control Protocol (MGCP) connection (**mgcp**)
- An **outbound** command denying access to Java applets (**nojava**)
- RPC connection (**rpc**)
- SIP connection (**sip**)
- Skinny Client Control Protocol (SCCP) connection (**skinny**)
- SMTP mail banner (**smtp_banner**)
- SMTP mail data (**smtp_data**)

- SQL*Net data fix up (**sqlnet_fixup_data**)
- Incomplete SMTP mail connection (**smtp_incomplete**)

protocol is a protocol that is specified by number. See the "Specifying Protocol Values" section in Appendix B, "Port and Protocol Values," for a list of valid protocol literal names.

The **show conn detail** command displays the following information:

```
{UDP | TCP} outside_ifc:real_addr/real-port [(map_addr/port)]
inside_ifc:real_addr/real_port [(map-addr/port)] flags flags
```

The connection flags are defined in Table 2-19.

Table 2-19 Connection Flags

Flag	Description
---	SKINNY (not used)
a	Awaiting outside ACK to SYN
A	Awaiting inside ACK to SYN
B	Initial SYN from outside
C	Computer Telephony Interface Quick Buffer Encoding (CTIQBE)
d	Dump
D	DNS
E	Outside back connection
f	Inside FIN
F	Outside FIN
g	Media Gateway Control Protocol (MGCP)
G	Group
h	H.225
H	H.323
i	Incomplete
I	Inbound data
k	RTP/RTCP (UDP) connection object
m	SIP media connection
M	SMTP data
O	Outbound data
p	Replicated (unused)
P	Inside back connection
q	SQL*Net data

Table 2-19 Connection Flags (continued)

Flag	Description
r	Inside acknowledged FIN
R	Outside acknowledged FIN
R	UDP RPC
s	Awaiting outside SYN
S	Awaiting inside SYN
t	SIP transient connection
T	TCP SIP connection
T	UDP SIP connection
U	Up

Examples

This example shows a TCP session connection from inside host 10.1.1.15 to the outside Telnet server at 192.150.49.10. Because there is no B flag, the connection is initiated from the inside. The U, I, and O flags indicate that the connection is active and has received inbound and outbound data.

```
fwsm(config)# show conn
2 in use, 2 most used
TCP out 192.150.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.150.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

This example shows a UDP connection from outside host 192.150.49.10 to inside host 10.1.1.15. The D flag indicates a DNS connection. The number 1028 is the DNS ID over the connection.

```
fwsm(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN,
       G - group, H - H.323, I - inbound data, M - SMTP data,
       O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, U - up
TCP outside:192.150.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.150.49.10/31649 inside:10.1.1.15/1028 flags dD
```

This example shows sample output from the **show conn** command:

```
show conn
6 in use, 6 most used
  TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
  TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
  TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
  TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
  TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
  TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
  UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
  UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
  UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

Host 10.3.3.4 on the inside has accessed a website at 209.165.201.1. The global address on the outside interface is 209.165.201.7.

This example shows how to display connections to the FWSM that are in the up state:

```
fwsm/context_name(config)# show conn state up
0 in use, 0 most used
 Network Processor 1 connections
 Network Processor 2 connections
```

Related Commands clear conn

show console-output

To display the currently configured console timeout value, use the **show console-output** command.

show console-output

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the console output:

```
fwsm(config)# show console-output
Message #1 : Initializing debugger......:  Message #2 : Found PCI card in slot:
 bus:2 dev:9 (vendor:0x8086 deviceid:0x1001)
Message #3 : Found PCI card in slot:2 bus:2 dev:8 (vendor:0x8086 deviceid:0x100
)
Message #4 : Found PCI card in slot:3 bus:1 dev:6 (vendor:0x1014 deviceid:0x1e8
Message #5 : Ignoring PCI card in slot:3 (vendor:0x1014 deviceid:0x1e8)
Message #6 : Found PCI card in slot:4 bus:1 dev:5 (vendor:0x1014 deviceid:0x1e8
Message #7 : Ignoring PCI card in slot:4 (vendor:0x1014 deviceid:0x1e8)
Message #8 : Found PCI card in slot:5 bus:1 dev:4 (vendor:0x1014 deviceid:0x1e8
Message #9 : Ignoring PCI card in slot:5 (vendor:0x1014 deviceid:0x1e8)
Message #10 : Found PCI card in slot:7 bus:0 dev:2 (vendor:0x1011 deviceid:0x22
Message #11 : PCI-2-PCI bridge in slot:7 (vendor:0x1011 deviceid:0x22)
Message #12 : IBM NP4GS3 in slot:7 dev:4 (vendor:0x1014 deviceid:0x1e8)
Message #13 : IBM NP4GS3 in slot:7 dev:5 (vendor:0x1014 deviceid:0x1e8)
Message #14 : IBM NP4GS3 in slot:7 dev:6 (vendor:0x1014 deviceid:0x1e8)
Message #15 : Found PCI card in slot:8 bus:0 dev:1 (vendor:0x1022 deviceid:0x20
0)
Message #16 : The NICs as we know them:
Message #17 : Nic 0: driver 2, bus 2, dev 9, irq 5, media 4, mediaIndex 0
Message #18 : Nic 1: driver 2, bus 2, dev 8, irq 7, media 4, mediaIndex 1
Message #19 : Nic 2: driver 3, bus 0, dev 1, irq 11, media 1, mediaIndex 0
Message #20 : write addr 0xa0000240, data 0x80000000
Message #21 : write addr 0xa0000240, data 0x80000000
Message #22 : write addr 0xa0000240, data 0x80000000
```

Related Commands

clear console-output

show context

To display the currently configured contexts, use the **show context** command.

show context [**detail**] [*name* | **admin** | **count**]

Syntax Description

detail	(Optional) Displays context details.
name	(Optional) Information about the specified context.
admin	(Optional) Displays the administrator context.
count	(Optional) Displays the number of contexts configured.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: Multiple

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display detailed information about the configured contexts:

```
fwsm/context_name(config)# show context my_context
Context Name      Class      Interfaces           URL
 my_context             default    30                   disk:my_context.cfg

fwsm/context_name(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    30,40                disk:admin.cfg
 my_context             default    30                   disk:my_context.cfg

fwsm/context_name(config)# show context count
Total active contexts: 2

fwsm(config)# changeto context my_context
fwsm/my_context(config)# show context
Context Name      Class      Interfaces           URL
 my_context             default    30                   disk:my_context.cfg
```

Related Commands

clear context
context

show counters

To display and clear the protocol stack counters, use the **show counters** command.

show counters [**context** *context-name* | **top** *N* | **all** | **summary**] [**protocol** *protocol_name* [**:***counter_name*]| **detail**] [**threshold** *count_threshold*]

Syntax Description

context	(Optional) Specifies a context.
context-name	(Optional) Context name.
top *N*	(Optional) Displays the counter details for the specified location.
all	(Optional) Displays the filter details.
summary	(Optional) Displays a counter summary.
protocol	(Optional) Displays the counters for the specified protocol.
protocol_name	(Optional) Protocol by name.
:*counter_name*	(Optional) Counter by name.
detail	(Optional) Displays the counters in detail.
threshold	(Optional) Displays only those counters at or above the specified threshold.
count_threshold	(Optional) Threshold to begin displaying counters.

Defaults

show counters summary detail threshold 1

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display all counters:

```
fwsm# show counters all
Protocol     Counter           Value   Context
IOS_IPC      IN_PKTS               2   single_vf
IOS_IPC      OUT_PKTS              2   single_vf

fwsm(config)# show counters
Protocol     Counter           Value   Context
NPCP         IN_PKTS            7195   Summary
NPCP         OUT_PKTS           7603   Summary
IOS_IPC      IN_PKTS             869   Summary
IOS_IPC      OUT_PKTS            865   Summary
IP           IN_PKTS             380   Summary
```

```
IP            OUT_PKTS             411   Summary
IP            TO_ARP               105   Summary
IP            TO_UDP                 9   Summary
UDP           IN_PKTS                9   Summary
UDP           DROP_NO_APP            9   Summary
FIXUP         IN_PKTS              202   Summary
```

This example shows how to display a summary of counters:

```
fwsm# show counters summary
Protocol      Counter            Value   Context
IOS_IPC       IN_PKTS                2   Summary
IOS_IPC       OUT_PKTS               2   Summary
```

This example shows how to display counters for a context:

```
fwsm# show counters context single_vf
Protocol      Counter            Value   Context
IOS_IPC       IN_PKTS                4   single_vf
IOS_IPC       OUT_PKTS               4   single_vf
```

Related Commands

clear counters

show cpu

To display the CPU utilization information, use the **show cpu usage** command.

In system context:

show cpu [**usage**] **context**

show cpu [**usage**] [**context** {**all** | *context_name*}]

In a context:

show cpu [**usage**]

Syntax Description

usage	(Optional) Displays the CPU usage for the FWSM.
context	(Optional) Specifies that the display shows contexts.
all	(Optional) Specifies that the display shows all context.
context_name	(Optional) Context name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show cpu usage** command displays the CPU usage information. When the command displays per-context CPU usage, the value is displayed with one decimal digit of precision instead of an integer value.

This command displays how the CPU usage is spread across all of the contexts and system-level (system and kernel) processes. The columns will always total 100 percent. In an idle system, all of the CPU usage is displayed in the system and kernel processes as shown in the examples.

In the system context:

- The **show cpu** command displays how busy the system currently is.
- The **show cpu context all** command displays where all the CPU time is being used.
- The **show cpu context** *context_name* command displays the percentage of CPU time used by the specified context.

In a context, the **show cpu** command displays the percentage of CPU time used by that context.

Examples

This example shows how to display the CPU utilization for the FWSM:

```
fwsm(config)# show cpu usage
CPU utilization for 5 seconds = 1%; 1 minute: 0%; 5 minutes: 0%
```

The percentage usage prints as NA (not applicable) if the usage is unavailable for the specified time interval. This situation can occur if you ask for CPU usage before the 5-second, 1-minute, or 5-minute time interval has elapsed.

This example shows how to display the CPU utilization for a context:

```
fwsm/context_name(config)# show cpu usage context admin
CPU utilization for 5 seconds = 1%; 1 minute: 0%; 5 minutes: 0%
```

This example shows how to display the CPU utilization for all contexts:

```
fwsm(config)# show cpu usage context all
CPU utilization for 5 seconds = 1%; 1 minute: 0%; 5 minutes: 0%
5 sec  1 min  5 min  Context Name
   0%     0%     0%  admin
  59%    59%    59%  system
  41%    41%    41%  <kernel>
```

show crashdump

To display the crash information file that is stored in the Flash partition of the FWSM, use the **show crashdump** command.

show crashdump [**save**]

Syntax Description

save	(Optional) Displays whether or not the FWSM is configured to save crash information to the Flash partition.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show crashdump save** command allows you to display whether or not the FWSM is configured to save crash information to the Flash partition.

The **show crashdump** command allows you to display the crash information file that is stored in the Flash partition of the FWSM. If the crash information file is from a test crash (from the **crashdump test** command), the first string of the crash information file is ": Saved_Test_Crash" and the last one is ": End_Test_Crash". If the crash information file is from a real crash, the first string of the crash information file is ": Saved_Crash" and the last one is ": End_Crash" (this includes crashes from the **crashdump force page-fault** or **crashdump force watchdog** commands).

Examples

This example shows how to display the current crash information configuration:

```
fwsm(config)# show crashdump save
crashdump save enable
```

This example shows the output for a crash information file test. (However, this test does not actually crash the FWSM. It provides a simulated example file.)

```
fwsm(config)# crashdump test
fwsm(config)# exit
fwsm(config)# show crashdump
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)
```

```
Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
.
.
.
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco Firewall Version 2.2
Cisco Device Manager Version 2.2

Compiled on Fri 15-Nov-02 14:35 by root

FWSM up 10 days 0 hours

Hardware:   FWSM, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This FWSM has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2002
```

```
------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2002

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

Interface vlan20 "", is administratively down, line protocol is up
        MAC address 0000.0000.0000, MTU 0
        IP address 127.0.0.1, subnet mask 255.255.255.255
                Received 0 packets, 0 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 0 packets
Interface vlan40 "outside", is up, line protocol is up
        MAC address 0005.9a38.7400, MTU 1500
        IP address 40.7.12.1, subnet mask 255.255.0.0
                Received 684499 packets, 473311321 bytes
                Transmitted 512981 packets, 29781306 bytes
                Dropped 0 packets
Interface vlan41 "inside", is up, line protocol is up
        MAC address 0005.9a38.7400, MTU 1500
        IP address 41.7.12.1, subnet mask 255.255.0.0
                Received 780297 packets, 70082987 bytes
                Transmitted 605699 packets, 473794675 bytes
                Dropped 61 packets
Interface vlan2000 "", is administratively down, line protocol is down
        MAC address 0000.0000.0000, MTU 0
        IP address 127.0.0.1, subnet mask 255.255.255.255
                Received 0 packets, 0 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 0 packets

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3792/4096 FragDBGC
```

```
.
.
.
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

Related Commands

clear crashdump
crashdump force

show crypto dynamic-map

To display a dynamic crypto map set, use the **show crypto dynamic-map** command.

show crypto dynamic-map [**tag** *dynamic-map-name*]

Syntax Description

tag *dynamic-map-name*	(Optional) Shows the crypto dynamic map set with the specified *map-name*.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

For detailed help, refer to the subcommand help in the mode where the commands are available. For example, you can enter the following:

```
fwsm/context_name(config)#  ca ?
fwsm(config)#  help ca.
```

Examples

This example shows sample output for the **show crypto dynamic-map** command:

```
fwsm(config)# show crypto dynamic-map
Crypto Engine Connection Map:
    size = 8, free = 7, used = 0, active = 0
```

The following partial configuration was in effect when the preceding **show crypto dynamic-map** command was issued:

```
crypto ipsec security-association lifetime seconds 120
crypto ipsec transform-set t1 esp-des esp-md5-hmac
crypto ipsec transform-set tauth ah-sha-hmac
crypto dynamic-map dyn1 10 set transform-set tauth t1
crypto dynamic-map dyn1 10 match address 152
crypto map to-firewall local-address Ethernet0
crypto map to-firewall 10 ipsec-isakmp
crypto map to-firewall 10 set peer 172.21.114.123
crypto map to-firewall 10 set transform-set tauth t1
crypto map to-firewall 10 match address 150
crypto map to-firewall 20 ipsec-isakmp dynamic dyn1
access-list 150 permit ip host 172.21.114.67 host 172.21.114.123
access-list 150 permit ip host 15.15.15.1 host 172.21.114.123
```

```
access-list 150 permit ip host 15.15.15.1 host 8.8.8.1
access-list 152 permit ip host 172.21.114.67 any
```

This example shows output from the **show crypto map** command for a crypto map named “mymap”:

```
fwsm(config)# show crypto map

Crypto Map: "mymap" interfaces: { outside }

Crypto Map "mymap" 1 ipsec-isakmp
        Peer = 171.69.231.241
        access-list no-nat; 1 elements
        access-list no-nat permit ip 192.168.0.0 255.255.255.0 1.1.1.0 255.255.255.0
(hitcnt=0)
        Current peer: 171.69.231.241
        Security association lifetime: 4608000 kilobytes/28800 seconds
        PFS (Y/N): Y
        DH group:  group5
        Transform sets={ mycrypt, }
```

Related Commands

clear crypto dynamic-map
crypto dynamic-map

show crypto engine

To display the cryptography engine usage statistics, use the **show crypto engine** command.

show crypto engine

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show crypto engine** command allows you to display the usage statistics for the cryptography engine that is used by the FWSM.

Examples

This example shows sample output for the **show crypto engine** command:

```
fwsm(config)# show crypto engine
Crypto Engine Connection Map:
    size = 8, free = 7, used = 0, active = 0
```

Related Commands

clear crypto dynamic-map

show crypto interface

To display the VPN accelerator cards (VACs) installed in the FWSM chassis and to display the packet, payload byte, queue length, and moving average counters for traffic moving through the card for VAC+, use the **show crypto interface** command.

show crypto interface [**counters**]

Syntax Description

counters	(Optional) Displays the packet count, byte queue, and moving averages for traffic through a VAC+.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show crypto interface** command allows you to display VACs that are installed in the FWSM chassis.

The **show crypto interface counters** command allows you to display information (see Table 2-20) for the FWSM VAC+ only.

Table 2-20 show crypto interface Counters

Counter	Description
interfaces	Number and type of crypto interface cards installed.
packet count	Number of packets sent to the installed crypto interface card(s).
payload bytes	Number of bytes of payload either after decapsulation or before encapsulation.
input queue (curr/max)	Total number of packets that are awaiting service from the crypto interface card(s).
interface queue (curr/max)	Total number of packets that have been queued at the crypto interface card(s) for service.

Table 2-20 show crypto interface Counters (continued)

Counter	Description
output queue (curr/max)	Total number of packets that have been released by the crypto interface card(s) and are awaiting dispatch to the packet path.
moving averages 5second 1minute 5minute	5-second, 1-minute, and 5-minute moving averages of the packet count and payload bytes through all crypto interface cards.

Examples

This example shows sample output from the **show crypto interface** and **show crypto interface counters** commands:

```
fwsm/context_name(config)# show crypto interface
Encryption hardware device : Crypto5823 (revision 0x1)
fwsm(config)# show crypto interface counters

interfaces: 1
  Crypto5823 (revision 0x1), maximum queue size 64

packet count:               318657093
payload bytes:              89861300946
input     queue (curr/max): 1336/1584
interface queue (curr/max): 64/64
output    queue (curr/max): 0/64
moving averages
  5second   128273 pkts/sec   289 Mbits/sec
  1minute   128326 pkts/sec   290 Mbits/sec
  5minute   128279 pkts/sec   289 Mbits/sec
```

This example shows the same sample output after the **clear crypto interface counters** command has been used:

```
fwsm/context_name(config)# clear crypto interface counters
fwsm/context_name(config)# show crypto interface counters

interfaces: 1
  Crypto5823 (revision 0x1), maximum queue size 64

packet count:               355968
payload bytes:              100382976
input     queue (curr/max): 1317/1537
interface queue (curr/max): 64/64
output    queue (curr/max): 0/64
moving averages
  5second       NA pkts/sec    NA Mbits/sec
  1minute       NA pkts/sec    NA Mbits/sec
  5minute       NA pkts/sec    NA Mbits/sec
```

This example shows sample output from the **show crypto interface** and **show crypto interface counters** commands when a VAC+ is installed:

```
fwsm/context_name(config)# show crypto interface
Encryption hardware device : IRE2141 with 2048KB, HW:1.0, CGXROM:1.9, FW:6.5
fwsm/context_name(config)# show crypto interface counters
no crypto interface counters available
```

This example shows sample output from the **show crypto interface** and **show crypto interface counters** commands when no crypto interface card is installed (neither a VAC nor a VAC+):

```
fwsm(config)# show crypto interface
fwsm(config)# show crypto interface counters
no crypto interface counters available
```

Related Commands

crypto map interface

show crypto ipsec

To display the configured transform sets, use the **show crypto ipsec** command.

show crypto ipsec security-association lifetime

show crypto ipsec transform-set [**tag** *transform-set-name*]

show crypto ipsec sa [**map** *map-name* | **address** | **identity**] [**detail**]

Syntax Description

security-association lifetime	Displays the security-association lifetime value that is configured for a crypto map entry.
transform-set	Displays the configured transform sets.
tag *transform-set-name*	(Optional) Specifies a transform set.
sa	Displays the settings that are used by the current security associations.
map *map-name*	(Optional) Name of the crypto map set.
address	(Optional) Displays all of the existing security associations, sorted by the destination address (either the local address or the address of the remote IPSec peer) and then by protocol (AH or ESP).
identity	(Optional) Displays only the flow information.
detail	(Optional) Displays detailed error counters.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show crypto ipsec sa** command allows you to display the settings that are used by the current security associations. If you do not enter a keyword, all security associations are displayed. They are sorted first by interface, and then by traffic flow (for example, source/destination address, mask, protocol, and port). Within a flow, the security associations are listed by protocol (ESP/AH) and direction (inbound/outbound). The **identity** keyword does not show the security association information.

Note While entering the **show crypto ipsec sa** command, if the screen display is stopped with the More prompt and the security association lifetime expires while the screen display is stopped, then the subsequent display may be outdated. In this situation, you should assume that the security association lifetime values that display are invalid.

The **show crypto ipsec sa** command allows you to display the Payload Compression Protocol (PCP) in its output.

Examples

This example shows how to display the security-association lifetime value:

```
fwsm/context_name(config)# show crypto ipsec security-association lifetime
Security-association lifetime: 4608000 kilobytes/120 seconds
```

This configuration was in effect when the preceding **show crypto ipsec security-association lifetime** command was issued:

```
fwsm/context_name(config)# crypto ipsec security-association lifetime seconds 120
```

This example shows how to display the configured transform sets:

```
fwsm/context_name(config)# show crypto ipsec transform-set

Transform set combined-des-sha: {  esp-des esp-sha-hmac  }
   will negotiate = {  Tunnel,  },

Transform set combined-des-md5: {  esp-des esp-md5-hmac  }
   will negotiate = {  Tunnel,  },

Transform set t1: { esp-des esp-md5-hmac  }
   will negotiate = {  Tunnel,  },

Transform set t100: {  ah-sha-hmac  }
   will negotiate = {  Tunnel,  },

Transform set t2: {  ah-sha-hmac  }
   will negotiate = {  Tunnel,  },
   {  esp-des  }
   will negotiate = {  Tunnel,  },
```

This configuration was in effect when the preceding **show crypto ipsec transform-set** command was issued:

```
fwsm/context_name(config)# crypto ipsec transform-set combined-des-sha esp-des
esp-sha-hmac
fwsm/context_name(config)# crypto ipsec transform-set combined-des-md5 esp-des
esp-md5-hmac
fwsm/context_name(config)# crypto ipsec transform-set t1 esp-des esp-md5-hmac
fwsm/context_name(config)# crypto ipsec transform-set t100 ah-sha-hmac
fwsm/context_name(config)# crypto ipsec transform-set t2 ah-sha-hmac esp-des
```

This example shows how to display the settings that are used by the current security associations:

```
fwsm/context_name(config)# show crypto ipsec sa

interface: outside
    Crypto map tag: firewall-alice, local addr. 172.21.114.123

   local  ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
```

```
    current_peer: 172.21.114.67
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
     #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
     #send errors 10, #recv errors 0

      local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67/500
      path mtu 1500, media mtu 1500
      current outbound spi: 20890A6F

      inbound esp sas:
       spi: 0x257A1039(628756537)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel UDP-Encaps, }
         slot: 0, conn id: 26, crypto map: firewall-alice
         sa timing: remaining key lifetime (k/sec): (4607999/90)
         IV size: 8 bytes
         replay detection support: Y
      inbound ah sas:
      outbound esp sas:
       spi: 0x20890A6F(545852015)
         transform: esp-des esp-md5-hmac ,
         in use settings ={Tunnel,  }
         slot: 0, conn id: 27, crypto map: firewall-alice
         sa timing: remaining key lifetime (k/sec): (4607999/90)
         IV size: 8 bytes
         replay detection support: Y
      outbound ah sas:
interface: inside
    Crypto map tag: firewall-alice, local addr. 172.21.114.123
    local ident (addr/mask/prot/port): (172.21.114.123/255.255.255.255/0/0)
    remote ident (addr/mask/prot/port): (172.21.114.67/255.255.255.255/0/0)
    current_peer: 172.21.114.67
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 10, #pkts encrypt: 10, #pkts digest 10
     #pkts decaps: 10, #pkts decrypt: 10, #pkts verify 10
     #send errors 10, #recv errors 0
      local crypto endpt.: 172.21.114.123, remote crypto endpt.: 172.21.114.67
      path mtu 1500, media mtu 1500
      current outbound spi: 20890A6F
        inbound esp sas:
       spi: 0x257A1039(628756537)
         transform: esp-des esp-md5-hmac  ,
         in use settings ={Tunnel,  }
         slot: 0, conn id: 26, crypto map: firewall-alice
         sa timing: remaining key lifetime (k/sec): (4607999/90)
         IV size: 8 bytes
         replay detection support: Y
      inbound ah sas:
      outbound esp sas:
       spi: 0x20890A6F(545852015)
         transform: esp-des esp-md5-hmac  ,
         in use settings ={Tunnel,  }
         slot: 0, conn id: 27, crypto map: firewall-alice
         sa timing: remaining key lifetime (k/sec): (4607999/90)
         IV size: 8 bytes
         replay detection support: Y
      outbound ah sas:
```

Related Commands

crypto ipsec security-association lifetime
crypto ipsec transform-set

show crypto map

To display the crypto map configuration, use the **show crypto map** command.

show crypto map [**interface** *interface-name* | **tag** *map-name*]

Syntax Description

interface *interface-name*	(Optional) Displays the identifying interface to be used by the FWSM to identify itself to peers.
tag *map-name*	(Optional) Displays the crypto map set with the specified map name.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the crypto map configuration:

```
fwsm/context_name(config)# show crypto map

Crypto Map: "firewall-alice" pif: outside local address: 172.21.114.123

Crypto Map "firewall-alice" 10 ipsec-isakmp
        Peer = 172.21.114.67
        access-list 141 permit ip host 172.21.114.123 host 172.21.114.67
        Current peer: 172.21.114.67
        Security-association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={  t1,  }
```

This configuration was in effect when the preceding **show crypto map** command was issued:

```
fwsm/context_name(config)# crypto map firewall-alice 10 ipsec-isakmp
fwsm/context_name(config)# crypto map firewall-alice 10 set peer 172.21.114.67
fwsm/context_name(config)# crypto map firewall-alice 10 set transform-set t1
fwsm/context_name(config)# crypto map firewall-alice 10 match address 141
```

This example shows the sample output for the **show crypto map** command when manually established security associations are used:

```
fwsm/context_name(config)# show crypto map

Crypto Map "multi-peer" 20 ipsec-manual
        Peer = 172.21.114.67
        access-list 120 permit ip host 1.1.1.1 host 1.1.1.2
        Current peer: 172.21.114.67
        Transform sets={  t2,  }
        Inbound esp spi: 0,
         cipher key: ,
         auth_key: ,
        Inbound ah spi: 256,
            key: 0102030405060708090102030405060708090102030405060708090,
        Outbound esp spi: 0
         cipher key: ,
         auth key: ,
        Outbound ah spi: 256,
            key: 0102030405060708090102030405060708090102030405060708090,
```

This configuration was in effect when the preceding **show crypto map** command was issued:

```
fwsm/context_name(config)# crypto map multi-peer 20 ipsec-manual
fwsm/context_name(config)# crypto map multi-peer 20 set peer 172.21.114.67
fwsm/context_name(config)# crypto map multi-peer 20 set session-key inbound ah 256
0102030405060708090102030405060708090102030405060708090
fwsm/context_name(config)# crypto map multi-peer 20 set session-key outbound ah 256
0102030405060708090102030405060708090102030405060708090
fwsm/context_name(config)# crypto map multi-peer 20 set transform-set t2
fwsm/context_name(config)# crypto map multi-peer 20 match address 120
```

Related Commands

crypto map client

show curpriv

To display the current user privileges, use the **show curpriv** command.

show curpriv

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

These examples show output from the **show curpriv** command when a user named enable_15 is at different privilege levels. The username indicates the name that the user entered when the user logged in, P_PRIV indicates that the user has entered the **enable** command, and P_CONF indicates that the user has entered the **config terminal** command.

```
fwsm(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
fwsm(config)# exit

fwsm(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
fwsm(config)#  exit

fwsm(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
fwsm(config)#
```

Related Commands

privilege
show privilege

show default-information originate

To display a type 7 default in the not-so-stubby area (NSSA), use the **show default-information originate** command.

show default-information originate

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command is supported on an NSSA ABR or an NSSA autonomous system boundary router (ASBR) only.

The **show ip ospf** command displays the configured **router ospf** subcommands.

Examples

This example shows how to display NSSA information:

```
fwsm/context_name(config)# show default-information originate
```

Related Commands

default-information originate (router OSPF subcommand)
router ospf
show ip ospf

show dbg

To display the debug information, use the **show dbg** command.

show dbg

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display debug information:

```
fwsm(config)# show dbg
i82557 isr
i82557 queues
ip config
ip open
ip close
ip put
ip get
ip ioctl
ip arpin
ip arpreq
ip in
ip answer
ip route
.
.
.
ci config
```

Related Commands

debug

show debug

To display the debug information, use the **show debug** command.

show debug

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display debug information:

```
fwsm(config)# show debug
```

Related Commands

debug

show dhcpd

To display the binding and statistics information associated with all of the **dhcpd** commands, use the **show dhcpd** command.

show dhcpd [**binding** | **statistics**]

Syntax Description

binding	(Optional) Displays binding information for a given server IP address and its associated client hardware address and lease length.
statistics	(Optional) Displays statistical information, such as the address pool, number of bindings, malformed messages, sent messages, and received messages.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example show how to display DHCPD statistics:

```
fwsm/context_name(config)# show dhcpd statistics
```

Related Commands

dhcpd
dhcprelay

show dhcprelay

To display the Dynamic Host Configuration Protocol (DHCP) relay statistics, use the **show dhcprelay** command.

show dhcprelay [**statistics**]

Syntax Description

statistics	(Optional) Displays counters for the packets that are relayed by the DHCP relay agent.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The output of the **show dhcprelay** command increments until you enter the **clear dhcprelay statistics** command.

Examples

This example show how to display DHCPD statistics:

```
fwsm/context_name(config)# show dhcprelay
```

Related Commands

clear dhcprelay
dhcpd
dhcprelay

show disk

To display the information about the disk file system, use the **show disk** command.

show disk all | filesys

Syntax Description

all	Displays all files in the file system and the geometry of the partitions.
filesys	Displays only the geometry of the partitions.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the disk file system information:

```
fwsm(config)# show disk
-#- --length-- -----date/time------ path
  1 1519       10:03:50 Jul 14 2003   my_context.cfg
  2 1516       10:04:02 Jul 14 2003   my_context.cfg
  3 1516       10:01:34 Jul 14 2003   admin.cfg

60973056 bytes available (12288 bytes used)
```

This example shows how to display all disk file system information and the partition information:

```
fwsm(config)# show disk all
-#- --length-- -----date/time------ path
  1 1519       10:03:50 Jul 14 2003   my_context.cfg
  2 1516       10:04:02 Jul 14 2003   my_context.cfg
  3 1516       10:01:34 Jul 14 2003   admin.cfg

60973056 bytes available (12288 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            8
   Number of Cylinders       467
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          119552
```

```
COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      59
   Sectors Per Cluster         8
   Number of Clusters      14889
   Number of Data Sectors 119264
   Base Root Sector          119
   Base FAT Sector             1
   Base Data Sector          151
```

This example shows how to display the partition information:

```
fwsm(config)# show disk filesys

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            8
   Number of Cylinders       467
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          119552

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      59
   Sectors Per Cluster         8
   Number of Clusters      14889
   Number of Data Sectors 119264
   Base Root Sector          119
   Base FAT Sector             1
   Base Data Sector          151
: Saved
```

show dispatch stats

To display all the dispatch layer statistics, use the **show dispatch stats** command.

show dispatch stats [**funcid**]

Syntax Description

funcid	(Optional) Specifies the dispatch layer statistics function ID.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the dispatch statistics table:

```
fwsm(config)# show dispatch stats

Dispatch Level Stats:
Total pkts received                       :         4855
Total bytes received                      :       332519
Total pkts dropped                        :            0
Total Control Channels Created            :            0
Total primary_sessions_created            :            0
Total secondary_sessions_created Created  :            0
Total sessions freed                      :            0
Total embryonic sessions created          :            0
Total session moved to full open          :            0
Total embryonic session timeouts          :            0
Total zombie created                      :            0
Total zombie reused                       :            0
Total zombie freed                        :            0
Max conn hash chain length                :            0
Total delete indications Received         :            0
Total buffer overflow count               :            0
Total url filtering connections       :            0

Fixup Error Stats:
Invalid Ethernet Type                     :            0
Packet Received in Indication             :            0
Invalid TLV Length                        :            0
Unknown TLV                               :            0
Invalid Packet Length                     :            0
Invalid L4 protocol in packet             :            0
Invalid conn ptr in indication            :            0
```

```
Unsolicited delete indication              :            0
Host object lookup failure for indication  :            0
Invalid internal interface in indication   :            0
Invalid PIF in session info TLV            :            0
Conn lookup failure for delte indication   :            0
Fragments received for missing conn object :            0
Session ID mismatch existing connection    :            0
Xlate ID mismatch for existing connnection :            0
Packets received for deleted connections   :            0

Connection object allocation failures      :            0
Host object allocation failures            :            0
Xlate allocation failures                  :            0
Xlate missing for conn                     :            0
full open in zombie                        :            0
Junk pointer in session TLV                        :            0
error in setting VCID                        :            0
```

Related Commands

clear dispatch stats

show dispatch table

To display all the dispatch layer statistics, use the **show dispatch table** command.

show dispatch table

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the dispatch statistics table:

```
fwsm(config)# show dispatch table
------------------------------------------------------------------------
                          NAT TABLE ENTRIES
 FID     CBACK FUNC    QUEUE       Channel    MAX_CONN   LINK STATUS
------------------------------------------------------------------------
   1      url_filter  TASK SWITCH    f682d0         1000      ACTIVE
   2          domain  FAST SWITCH    f684b0         1000      ACTIVE
   4             ftp  FAST SWITCH    f684b0         1000      ACTIVE
   5            http  TASK SWITCH    f68258         1000      ACTIVE
   6       h323_h225  TASK SWITCH    f68280         1000      ACTIVE
   7        h323_ras  TASK SWITCH    f68398         1000      ACTIVE
   8             ils  FAST SWITCH    f684b0         1000      ACTIVE
   9             rpc  FAST SWITCH    f684b0         1000      ACTIVE
  10             rsh  TASK SWITCH    f68294         1000      ACTIVE
  11            rtsp  TASK SWITCH    f682e4         1000      ACTIVE
  12            smtp  FAST SWITCH    f684b0         1000      ACTIVE
  13          sqlnet  TASK SWITCH    f682a8         1000      ACTIVE
  14             sip  TASK SWITCH    f68320         1000      ACTIVE
  15          skinny  TASK SWITCH    f68334         1000      ACTIVE
  16      udp_domain  FAST SWITCH    f684b0         1000      ACTIVE
  17         rpc_udp  FAST SWITCH    f684b0         1000      ACTIVE
  18           xdmcp  FAST SWITCH    f684b0         1000      ACTIVE
  19         udp_sip  TASK SWITCH    f683fc         1000      ACTIVE
  20         netbios  FAST SWITCH    f684b0         1000      ACTIVE
  21    ftp_filter_command  TASK SWITCH    f68438         1000      ACTIVE
  22    https_filter  TASK SWITCH    f6844c         1000      ACTIVE
  23             mgcp  TASK SWITCH    f68474         1000      ACTIVE
  33    indication handler  TASK SWITCH    f684c4         1000      ACTIVE
  34      AAA/events  TASK SWITCH    f684d8         1000      ACTIVE
```

```
  35         np/show  TASK SWITCH    f684ec         1000      ACTIVE
  36    pkt to IPstack  TASK SWITCH    f68500         1000      ACTIVE
  37    syslog_entry  TASK SWITCH    f68514         1000      ACTIVE
  38    fornax_pk_lu_process  TASK SWITCH    f68528         1000      ACTIVE
-------------------------------------------------------------------------
                            PAT TABLE ENTRIES

 FID    CBACK FUNC     QUEUE       Channel     MAX_CONN   LINK STATUS
-------------------------------------------------------------------------
 129     url_filter  TASK SWITCH    f682d0         1000      ACTIVE
 130         domain  TASK SWITCH    f6830c         1000      ACTIVE
 132            ftp  FAST SWITCH    f684b0         1000      ACTIVE
 133           http  TASK SWITCH    f68258         1000      ACTIVE
 134      h323_h225  TASK SWITCH    f68280         1000      ACTIVE
 135       h323_ras  TASK SWITCH    f68398         1000      ACTIVE
 136            ils  TASK SWITCH    f68348         1000      ACTIVE
 137            rpc  TASK SWITCH    f68460         1000      ACTIVE
 138            rsh  TASK SWITCH    f68294         1000      ACTIVE
 140           smtp  TASK SWITCH    f6826c         1000      ACTIVE
 141         sqlnet  TASK SWITCH    f682a8         1000      ACTIVE
 142            sip  TASK SWITCH    f68320         1000      ACTIVE
 143         skinny  TASK SWITCH    f68334         1000      ACTIVE
 144     udp_domain  TASK SWITCH    f68410         1000      ACTIVE
 145        rpc_udp  TASK SWITCH    f68370         1000      ACTIVE
 146          xdmcp  TASK SWITCH    f68384         1000      ACTIVE
 147        udp_sip  TASK SWITCH    f683fc         1000      ACTIVE
 148        netbios  TASK SWITCH    f683d4         1000      ACTIVE
 149   ftp_filter_command  TASK SWITCH    f68438         1000      ACTIVE
 150   https_filter  TASK SWITCH    f6844c         1000      ACTIVE
-------------------------------------------------------------------------
```

Related Commands

clear dispatch stats
show dispatch stats

show distance

To display the OSPF route administrative distances based on route type, use the **show distance** command.

show distance

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display OSPF route administrative distances:

```
fwsm(config)# show distance
```

Related Commands

distance (router submode)
router ospf
show ip ospf

show domain-name

To display the IPSec domain name, use the **show domain-name** command.

show domain-name *name*

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **domain-name** command allows you to change the IPSec domain name.

Note The change of the domain name causes the change of the fully qualified domain name. Once the fully qualified domain name is changed, delete the RSA key pairs using the **ca zeroize rsa** command, and delete related certificates using the **no ca identity** *ca_nickname* command.

Examples

This example shows how to display the IPSec domain name:

```
fwsm/context_name(config)# show domain-name example.com
```

Related Commands

domain-name

show dynamic-map

To display a dynamic crypto map entry, use the **show dynamic-map** command.

show dynamic-map

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the dynamic crypto map entries:

```
fwsm/context_name(config)# show dynamic-map
No crypto map templates found.
```

Related Commands

crypto dynamic-map
dynamic-map

show enable

To display the password configuration for privilege levels, use the **show enable** command.

show enable

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the password configuration:

```
fwsm/context_name(config)# show enable
enable password 8Ry2YjIyt7RRXU24 encrypted
```

Related Commands

enable

show established

To display the allowed inbound connections that are based on established connections, use the **show established** command.

show established

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display inbound connections that are based on established connections:

```
fwsm/context_name(config)# show established
```

Related Commands

clear established
established

show failover

To verify the status of the connection and to determine which module is active, use the **show failover** command.

show failover [**statistics** | **state** | **interface** | **history**]

Syntax Description

statistics	Displays failover statistics.
state	Displays the failover state.
interface	Displays the interface configuration.
history	Displays the configuration history.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.3(1)	Support for the Autostate feature and suspend configuration synchronization were added on the FWSM.

Usage Guidelines

The **show failover** command allows you to display the dynamic failover information, interface status, and logical interface update status. In the **show failover** output, the fields have the following values:

- Stateful Obj has these values:
  - Xmit—Indicates the number of packets transmitted.
  - Xerr—Indicates the number of transmit errors.
  - Rcv—Indicates the number of packets received.
  - Rcv—Indicates the number of receive errors.
- Each row is for a particular object static count as follows:
  - General—Indicates the sum of all stateful objects.
  - Sys cmd—Refers to the logical update system commands, such as **login** or **stay alive**.
  - Up time—Indicates the value for the FWSM up time, which the active FWSM module will pass on to the standby module.
  - Xlate—Indicates the FWSM translation information.
  - Tcp conn—Indicates the FWSM dynamic TCP connection information.

- Udp conn—Indicates the FWSM dynamic UDP connection information.
- ARP tbl—Indicates the FWSM dynamic ARP table information.
- RIF tbl—Indicates the dynamic router table information.

The Standby Logical Update Statistics output that is displayed when you use the **show failover** command describes only the stateful failover. The "xerrs" value does not indicate an error in failover, but rather the number of packet transmit errors.

If you do not enter a failover IP address, the **show failover** command displays 0.0.0.0 for the IP address, and monitoring of the interfaces remain in a "waiting" state. You must set a failover IP address for failover to work.

Autostate allows the FWSM to quickly detect the failure of the interfaces connecting the real hosts. To allow autostate support on an FWSM interface, you must enable interface monitoring (see the **monitor-interface** command) on that interface. The switch operating system software informs the FWSM when the first or last physical port has joined or left a VLAN assigned to that FWSM, excluding the FWSM port channel and trunk port to the MSFC.

The FWSM responds to a VLAN down condition by marking the interfaces associated with that VLAN as autostate down. This VLAN is considered as a failed interface for interface monitoring of health status and may cause a failover if the interface policy threshold is met. When suspend configuration configuration is enabled, two interfaces will no longer synchronize the configuration or replicate commands.

Note When suspend configuration synchronization is enabled, interface monitoring and logical interfaces are disabled.

Examples

This example shows how to display failover information. See Table 2-21 for a description of each field.

```
fwsm(config)# show failover
Failover On
Failover unit Primary
Failover LAN Interface fover Vlan 150
Unit Poll frequency 15 seconds
Interface Poll frequency 15 seconds
Interface Policy 50%
Monitored Interfaces 249 of 250 maximum
Config sync: active
Last Failover at: 10:58:08 Apr 15 2004
        This host: Primary - Active
                Active time: 2232 (sec)
                admin Interface inside (10.6.8.91): Normal
                admin Interface outside (70.1.1.2): Normal
        Other host: Secondary - Standby
                Active time: 0 (sec)
                admin Interface inside (10.6.8.100): Normal
                admin Interface outside (70.1.1.3): Normal

Stateful Failover Logical Update Statistics
        Link : Luifc Vlan 151
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         0          0          0          0
        up time         0          0          0          0
        xlate           0          0          0          0
        tcp conn        0          0          0          0
        udp conn        0          0          0          0
```

```
ARP tbl          0           0           0           0
RIP Tbl          0           0           0           0

Logical Update Queue Information
                 Cur     Max     Total
Recv Q:          0       0       0
Xmit Q:          0       0       0
```

Table 2-21 describes the **show failover** output.

Table 2-21 Show Failover Display Description

Field	Options
Failover	• On • Off
Failover Unit	• Primary • Secondary
Failover LAN Interface	Shows the interface name and VLAN for the failover link: *interface_name* **vlan** *number* If you have not configured the failover interface, the display shows: `Not configured`
Unit Poll frequency	*n* seconds The number of seconds that you set with the **failover poll unit** command. The default is 15 seconds.
Interface Poll frequency	*n* seconds The number of seconds that you set with the **failover poll interface** command. The default is 15 seconds.
Interface Policy	*n*[%] The threshold for interface failure that you set with the **failover interface-policy** command. The default is 50%.
Monitored Interfaces	*n* of 250 maximum The number of interfaces that you are monitoring.
Config sync	• Active—Configuration synchronization is active on the FWSM • Suspended—Configuration synchronization has been suspended or disabled on the FWSM
Last Failover	The last time that a failover occurred.
This host: Other host:	For each host, the display shows the following information.

Table 2-21 Show Failover Display Description (continued)

Field	Options
Primary or Secondary	• Active—The unit is in active mode. • Standby—The unit is in standby mode, • Disabled—The unit has failover disabled, or the failover link is not configured. • Listen—The unit is attempting to discover an active unit by listening for polling messages. • Learn—The unit detected an active unit, and is not synchronizing the configuration before going to standby mode. • Failed—The unit is failed.
Active time:	*n* (sec) The amount of time that the unit has been in the active state. This time is cumulative, so the standby unit, if it was active in the past, will also show a value.
[*context_name*] Interface *name* (*n.n.n.n*):	For each interface, the display shows the IP address currently being used on each unit, as well as one of the following conditions: • Failed—The interface has failed. • Link Down—The interface line protocol is down. • Normal—The interface is working correctly. • No Link—The interface has been administratively shut down. • Unknown—The FWSM cannot determine the status of the interface. • (Waiting)—The interface has not yet received any polling messages from the other unit. • (Autostate Down)—The interface is marked as autostate down. • Testing—The interface is being tested. In multiple context mode, the context name appears before each interface.
Stateful Failover Logical Update Statistics	The following fields relate to the stateful failover feature. If the Link field shows an interface name, the stateful failover statistics are shown.
Link	• *interface_name*—The interface used for the stateful failover link. • Unconfigured—You are not using stateful failover.
Stateful Obj	For each field type, the following statistics are used: • xmit—Number of transmitted packets to the other unit. • xerr—Number of errors that occurred while transmitting packets to the other unit. • rcv—Number of received packets. • rerr—Number of errors that occurred while receiving packets from the other unit.
General	Sum of all stateful objects.

Table 2-21 Show Failover Display Description (continued)

Field	Options
sys cmd	Logical update system commands; for example, LOGIN and Stay Alive.
up time	Up time, which the active unit passes to the standby unit.
xlate	Translation information.
tcp conn	TCP connection information.
udp conn	Dynamic UDP connection information.
ARP tbl	Dynamic ARP table information.
RIP Tbl	Dynamic router table information.
Logical Update Queue Information	For each field type, the following statistics are used: • Cur—Current number of packets • Max—Maximum number of packets • Total—Total number of packets
Recv Q	Status of the receive queue.
Xmit Q	Status of the transmit queue.

Related Commands

clear failover
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover reset
monitor-interface
show failover
write standby

show file

To display the information about the file system, use the **show file** command.

show file descriptors | system

Syntax Description

descriptors	Displays all open file descriptors.
system	Displays the size, bytes available, type of media, flags, and prefix information about the disk file system.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the file system information:

```
fwsm(config)# show file descriptors
No open file descriptors
fwsm(config)# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

Related Commands

cd
copy disk
copy flash
copy tftp
copy tftp
dir
format
mkdir
more
pwd
rename
rmdir

show filter

To display the URL, Java, or HTTPS filtering information, use the **show filter** command.

show filter

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display filtering information:

```
fwsm/context_name(config)# show filter
```

Related Commands

clear filter
filter ftp
filter https
filter url

show firewall

To display the FWSM mode, use the **show firewall** command.

show firewall [**transparent**]

Syntax Description

transparent	(Optional) Specifies the transparent mode.

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the firewall mode:

```
fwsm(config)# show firewall
Firewall mode: Router
```

Related Commands

clear firewall
firewall

show fixup

To display the fixup configuration and port values, use the **show fixup** command.

show fixup

show fixup protocol {*protocol* [*protocol*] | **mgcp**}

Syntax Description

protocol *protocol*	(Optional) Displays the port values for the protocol specified.
mgcp	(Optional) Displays the configured MGCP fixups.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show fixup** command allows you to display the current fixup configuration and port values.

The **show fixup protocol** *protocol* [*protocol*] command allows you to display the port values for the individual protocol specified.

The **show fixup protocol mgcp** command allows you to display the configured MGCP fixups.

Examples

This example shows how to display the current fixup configuration and port values:

```
fwsm(config)# show fixup
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol pptp 1723
fixup protocol sip udp 5060
```

This example shows the configured MGCP fixups:

```
fwsm(config)# show fixup protocol mgcp
fixup protocol mgcp 2427
fixup protocol mgcp 2727
```

Related Commands

clear fixup
fixup protocol

show flashfs

To display the file system information, use the **show flashfs** command.

show flashfs

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show flashfs** command displays the size in bytes of each file system sector and the current state of the file system. The data in each sector is as follows:

- file 0—FWSM binary image, where the .bin file is stored.
- file 1—FWSM configuration data that you can view with the **show config** command.
- file 2—FWSM data file that stores IPSec key and certificate information.
- file 3—flashfs downgrade information for the **show flashfs** command.
- file 4—The compressed FWSM image size in the Flash partition.

The origin values are integer multiples of the underlying file system sector size.

Examples

This example shows how to display file system information:

```
fwsm(config)# show flashfs
flash file system:  version:2  magic:0x12345679
  file 0: origin:       0 length:1511480
  file 1: origin: 2883584 length:3264
  file 2: origin:       0 length:0
  file 3: origin: 3014656 length:4444164
  file 4: origin: 8257536 length:280
```

Related Commands

clear floodguard
clear flashfs
no flashfs

show floodguard

To display the flood guard status, use the **show floodguard** command.

show floodguard

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the flood guard status:

```
fwsm/context_name(config)# show floodguard
floodguard enable
```

Related Commands

clear floodguard
floodguard

show fragment

To display the states of the fragment databases, use the **show fragment** command.

show fragment [*interface*]

Syntax Description

interface	(Optional) FWSM interface.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show fragment** command allows you to display the states of the fragment databases. If you specify the interface name, only information for the database residing at the specified interface is displayed. If you do not specify the interface name, the command will apply to all interfaces.

Use the **show fragment** command to display this information:

- State of the fragment database.
- Size—Maximum number of packets set by the **size** keyword. This value is the maximum number of fragments that are allowed on the interface. (Max_Block)
- Chain—Maximum number of fragments for a single packet set by the **chain** keyword. (Max_Block_Chain)
- Timeout—Maximum number of seconds set by the **timeout** keyword. This value is the time that you allow the fragments to exist in the system per interface before they are deleted by the garbage collection process.
- Queue—Number of packets currently awaiting reassembly. This value specifies the actual number of fragments that have been received on the interface. (Block_Queued)
- Assemble—Number of packets successfully reassembled. This counter is not used because the FWSM is providing virtual reassembly of packets.
- Fail—Number of packets that failed to be reassembled. This error counter is incremented when bad fragments are received.
- Overflow—Number of packets that overflowed the fragment database. This counter is incremented when the limit that you specify for fragmented packets crossing the interface is reached.

Examples

This example shows how to display the states of the fragment databases:

```
fwsm(config)# show fragment outside
Interface:outside
Size:2000, Chain:45, Timeout:10
Queue:1060, Assemble:809, Fail:0, Overflow:0
```

Related Commands

clear fragment
fragment

show ftp

To display the FTP mode, use the **show ftp** command.

show ftp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the FTP mode:

```
fwsm(config)# show ftp
ftp mode passive
```

Related Commands

clear ftp
ftp mode

show gc

To display the garbage collection process statistics, use the **show gc** command.

show gc

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display garbage collection process statistics:

```
fwsm(config)# show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

Related Commands

clear gc

show global

To display the **global** commands in the configuration, use the **show global** command.

show global

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the global commands:

```
fwsm/context_name(config)# show global
```

Related Commands

clear global
global

show h225

To display the **H225** statistics, use the **show h225** command.

show h225

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the H225 statistics:

```
fwsm/context_name(config)# show h225
Total: 0
        LOCAL           TPKT    FOREIGN         TPKT
```

Related Commands

show h245
show h323-ras

show h245

To display the H245 statistics, use the **show h245** command.

show h245

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This command shows how to display the H245 statistics:

```
fwsm/context_name(config)# show h245
Total: 0
        LOCAL           TPKT    FOREIGN         TPKT
```

Related Commands

show h225
show h323-ras

show h323-ras

To display the H323-ras statistics, use the **show h323-ras** command.

show h323-ras

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This command shows how to display the H323-ras statistics:

```
fwsm/context_name(config)# show h323-ras
Total: 0
        GK              Caller
```

Related Commands

show h225
show h245

show history

To display the previously entered commands, use the **show history** command.

show history

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show history** command allows you to display previously entered commands. You can examine commands individually with the up and down arrows, enter **^p** to display previously entered lines, or enter **^n** to display the next line.

Examples

This example shows how to display previously entered commands when you are in unprivileged mode:

```
fwsm> show history
    show history
    help
    show history
```

This example shows how to display previously entered commands when you are in privileged mode:

```
fwsm/context_name(config)# show history
    show history
    help
    show history
    enable
    show history
```

This example shows how to display previously entered commands when you are in configuration mode:

```
fwsm(config)# show history
    show history
    help
    show history
    enable
    show history
    config t show history
```

show hostname

To display the host name in the FWSM command line prompt, use the **show hostname** command.

show hostname

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display a host name:

```
fwsm(config)# show hostname
fwsm(config)#
```

Related Commands

hostname
clear hostname

show http

To display the HTTP server information, use the **show http** command.

show http

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display HTTP server information:

```
fwsm/context_name(config)# show http
http server disabled
```

Related Commands

clear http
http

show hw

To display the FWSM hardware version, use the **show hw** command.

show hw

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the FWSM hardware version:

```
fwsm/context_name(config)# show hw

FWSM Firewall Version 2.2(0)141

c6000-fwm-2-1-0-141  #126: Wed Jun 18 16:31:27 MDT 2003
    msgreene@boulder-view3:/users/msgreene/projects/firecat/mainline/XFWSM/obj

sw8fx1 up 1 hour 9 mins
Configuration last modified by enable_15 at 12:46:55 Jul 18 2003
```

Related Commands

show version

show icmp

To display the ICMP information, use the **show icmp** command.

show icmp

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display ICMP information:

```
fwsm/context_name(config)# show icmp
icmp permit any mgmt
```

Related Commands

icmp
clear icmp

show igmp

To display the Internet Group Management Protocol (IGMP) information for a multicast group, whether statically configured or dynamically created, use the **show igmp** command.

show igmp [*group* | **interface** *interface_name*] [**detail**]

Syntax Description

group	(Optional) Address of the multicast group to join.
interface *interface_name*	(Optional) Specifies the name of the interface to display information.
detail	(Optional) Displays all information in the IGMP table.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: System

Command Mode: Global

Command History

Release	Modification
	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the IGMP information for a multicast group:

```
fwsm(config)# show igmp

  IGMP is enabled on interface inside
  Current IGMP version is 2
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
  Inbound IGMP access group is
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 10.1.3.1 (this system)

  IGMP Connected Group Membership
   Group Address    Interface            Uptime    Expires   Last Reported
```

Related Commands

show multicast

show ignore lsa mospf

To display the link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets that you did not want sent to the syslog, use the **show ignore lsa mospf** subcommand.

show ignore lsa mospf

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the link-state advertisement (LSA) for type 6 Multicast OSPF (MOSPF) packets that you do not want to syslog:

```
fwsm/context_name(config)# show ignore lsa mospf
```

Related Commands

ignore lsa mospf (router ospf submode)
router ospf
show ip ospf

show interface

To display the information about the VLAN configuration, use the **show interface** command.

show interface [*interface*] [**running-config** | **detail** | **stats** | {**ip** [**brief**]}]

Syntax Description

interface	(Optional) Interface; see the "Usage Guidelines" section for additional information.
running-config	(Optional) Displays the interface running configuration.
detail	(Optional) Displays the interface configuration details.
stats	(Optional) Displays the interface statistics.
ip	(Optional) Displays information about the interface IP configuration.
brief	(Optional) Displays compacted information about the interface IP configuration.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You can use this command to display the status of interfaces. You can specify the *id* (as either the VLAN or the mapped name) or the name of the interface. The *interface* argument identifies a particular interface.

The dropped packets statistic in the display shows a record of those packets that arrived on the interface, but were not destined for the FWSM. These packets include traffic flooded by the switch, multicast and broadcast traffic (unless the FWSM is configured to relay those) and packets that fail sanity checks such as incorrect IP length versus Layer 2 length or checksums. This counter does not record packets dropped by the security policy.

Examples

This example shows how to display the interface activity:

```
fwsm(config)# show interface
Interface int450 "", is administratively down, line protocol is up
        Available but not configured via nameif
Interface int901 "share1", is administratively down, line protocol is down
        Available but not assigned from Supervisor
        MAC address 0005.9a38.7400, MTU 1500
        IP address 1.1.1.1, subnet mask 255.255.0.0
```

```
                Received 0 packets, 0 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 0 packets
Interface int902 "", is administratively down, line protocol is down
        Available but not assigned from Supervisor or configured via nameif
Interface Vlan10 "mgmt", is up, line protocol is up
        MAC address 0005.9a38.7400, MTU 1500
        IP address 10.7.12.1, subnet mask 255.255.0.0
                Received 565 packets, 109547 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 812 packets
Interface Vlan40 "outside", is administratively down, line protocol is up
        MAC address 0005.9a38.7400, MTU 1500
        IP address 40.7.12.1, subnet mask 255.255.0.0
                Received 0 packets, 0 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 0 packets
Interface Vlan41 "inside", is administratively down, line protocol is down
        MAC address 0005.9a38.7400, MTU 1500
        IP address 41.7.12.1, subnet mask 255.255.0.0
                Received 0 packets, 0 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 0 packets
In this context:
int450 = vlan450 - trunked from the cat6k, but no nameif has been done
int901 = vlan901 - NOT trunked from cat6k and a nameif has been done
int902 = vlan902 - NOT trunked from cat6k but no nameif has been done
vlan10 - trunked and nameif'd
vlan40 - trunked and namei'd, but shut
vlan41 - trunked and nameif'd, but the vlan has been shut from system.
fwsm(config)#
```

This example shows how to display the interface statistics:

```
fwsm(config)# show interface vlan10 stats
Interface vlan10 "", is administratively down, line protocol is up
        MAC address 0000.0000.0000, MTU 0
        IP address 127.0.0.1, subnet mask 255.255.255.255
                Received 0 packets, 0 bytes
                Transmitted 0 packets, 0 bytes
                Dropped 0 packets
```

Related Commands

clear interface stats
interface

show ip address

To display the IP addresses that are assigned to the network interfaces, use the **show ip address** command.

show ip address [*interface_name*]

Syntax Description

interface_name	(Optional) Interface name to display detailed information; valid values are **dhcp** and **pppoe**.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **dhcp** keyword displays detailed information about the Dynamic Host Configuration Protocol (DHCP) lease.

The **pppoe** keyword displays detailed information about the Point-to-Point Protocol Over Ethernet (PPPOE) connection.

Examples

This example shows how to display the IP addresses assigned to the network interfaces:

```
fwsm(config)# show ip address
System IP Addresses:
        ip address outside 209.165.201.2 255.255.255.224
        ip address inside 192.168.2.1 255.255.255.0
        ip address perimeter 192.168.70.3 255.255.255.0
Current IP Addresses:
        ip address outside 209.165.201.2 255.255.255.224
        ip address inside 192.168.2.1 255.255.255.0
        ip address perimeter 192.168.70.3 255.255.255.0
```

The current IP addresses are the same as the system IP addresses on the failover active module. When the primary module fails, the current IP addresses become the IP addresses of the standby module.

Related Commands

clear ip address
clear ip verify reverse-path
ip address
ip prefix-list
ip verify reverse-path
show ip address
show ip verify

show ip ospf

To display the general information about the OSPF routing processes, use the **show ip ospf** command.

show ip ospf [*pid*]

Syntax Description

pid	(Optional) ID of the OSPF process.

Defaults

Lists all OSPF processes if no *pid* is specified.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

If the *pid* is included, only information for the specified routing process is included.

Examples

These examples show how to display general information about the OSPF routing processes:

```
fwsm(config)# show ip ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
fwsm(config)# show ip ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
```

```
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0

Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x     0
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 0. 0 normal 0 stub 0 nssa
External flood list length 0
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf border-routers

To display the internal OSPF routing table entries to an area border router (ABR) and autonomous system boundary router (ASBR), use the **show ip ospf border-routers** command.

show ip ospf border-routers

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display the internal OSPF routing table entries to an ABR and ASBR:

```
fwsm/context_name(config)# show ip ospf border-routers
OSPF Process 5 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
OSPF Process 12 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf database

To display the lists of information that are related to the Open Shortest Path First (OSPF) database for a specific router, use the **show ip ospf database** command.

show ip ospf [*pid*] **database** [**internal**] [**adv-router** [*addr*]]

show ip ospf [*pid* [*area_id*]] **database** [**internal**] [**self-originate**] [*lsid*]

show ip ospf [*pid* [*area_id*]] **database** {**router** | **network** | **summary** | **asbr-summary** | **external** | **nssa-external** | **database-summary**}

Syntax Description

pid	(Optional) ID of the OSPF process.
database	Displays the database information.
internal	(Optional) Displays the routes that are internal to a specified autonomous system.
adv-router	(Optional) Displays the advertised router.
addr	(Optional) Router address.
area_id	(Optional) ID of the area that is associated with the OSPF address range.
self-originate	(Optional) Displays the information for the specified autonomous system.
lsid	(Optional) LSA ID.
router	(Optional) Displays the router.
network	(Optional) Displays the OSPF database information about the network.
summary	(Optional) Displays a summary of the list.
asbr-summary	(Optional) Displays an ASBR list summary.
external	(Optional) Displays the routes external to a specified autonomous system.
nssa-external	(Optional) Displays the external not-so-stubby-area list.
database-summary	(Optional) Displays the complete database summary list.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

The various forms of this command deliver information about different OSPF LSAs.

If you intend to associate the areas with IP subnets, you can specify a subnet address as the *area_id* using the following guidelines:

- When used in the context of authentication, *area_id* is the identifier of the area on which authentication is to be enabled.
- When using a cost context, *area_id* is the identifier for the stub or not-so-stubby are (NSSA).
- When used in the context of a prefix list, *area_id* is the identifier of the area on which filtering is configured.
- When used in a stub area or NSSA context, *area_id* is the identifier for the stub or NSSA area.
- When used in the context of an area range, *area_id* is the identifier of the area at whose boundary to summarize routes.

Examples

This example shows how to display the lists of information that are related to the OSPF database for a specific router:

```
fwsm/context_name(config)# show ip ospf database router
OSPF Router with ID (127.0.0.1) (Process ID 5)
OSPF Router with ID (172.23.59.232) (Process ID 12)
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf flood-list

To display a list of OSPF link-state advertisements (LSAs) waiting to be flooded over an interface, use the **show ip ospf flood-list** command.

show ip ospf flood-list *interface_name*

Syntax Description

interface_name	Name of the interface for which to display neighbor information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display a list of OSPF LSAs waiting to be flooded over an interface:

```
fwsm/context_name(config)# show ip ospf flood-list outside
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf interface

To display the OSPF-related interface information, use the **show ip ospf interface** command.

show ip ospf interface *interface_name*

Syntax Description

interface_name	Name of the interface for which to display the OSPF-related information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display the OSPF-related interface information:

```
fwsm/context_name(config)# show ip ospf interface
fwsm/context_name(config)# show ip ospf interface inside
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf neighbor

To display the OSPF-neighbor information on a per-interface basis, use the **show ip ospf neighbor** command.

show ip ospf neighbor [*interface_name*] [*nbr_router_id*] [**detail**]

Syntax Description

interface_name	(Optional) Name of the interface for which to display neighbor information.
nbr_router_id	(Optional) ID of the neighbor router.
detail	(Optional) Lists all neighbors.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display the OSPF-neighbor information on a per-interface basis:

```
fwsm/context_name(config)# show ip ospf neighbor outside detail
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf request-list

To display a list of all link-state advertisements (LSAs) that are requested by a router, use the **show ip ospf request-list** command.

show ip ospf request-list *nbr_router_id interface_name*

Syntax Description

nbr_router_id	ID of the neighbor router that is specified by its IP address. Displays the list of all LSAs that are requested by the router from this neighbor.
interface_name	Name of the interface for which to display neighbor information. Displays the list of all LSAs that are requested by the router from this interface.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display a list of LSAs that are requested by a router:

```
fwsm/context_name(config)# show ip ospf request-list 172.23.59.232 outside
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf retransmission-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf retransmission-list

To display a list of all link-state advertisements (LSAs) waiting to be resent, use the **show ip ospf retransmission-list** command.

show ip ospf retransmission-list *nbr_router_id interface_name*

Syntax Description

nbr_router_id	ID of the neighbor router that is specified by its IP address.
interface_name	Name of the interface for which to display neighbor information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

The *nbr_router_id* argument displays the list of all LSAs that are waiting to be resent for this interface.

The *interface_name* argument displays the list of all LSAs that are waiting to be resent for this neighbor.

Examples

This example shows how to display a list of all LSAs that are waiting to be resent:

```
fwsm/context_name(config)# show ip ospf retransmission-list 173.25.26.201 outside
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf summary-address
show ip ospf virtual-links
show routing

show ip ospf summary-address

To display a list of all summary address redistribution information that is configured under an OSPF process, use the **show ip ospf summary-address** command.

show ip ospf summary-address

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display a list of all summary address redistribution information before a summary address has been configured for an OSPF process with the ID of 5:

```
fwsm/context_name(config)# show ip ospf 5 summary-address
OSPF Process 5, Summary-address
    Not configured
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf virtual-links
show routing

show ip ospf virtual-links

To display the parameters and the current state of OSPF virtual links, use the **show ip ospf virtual-links** command.

show ip ospf virtual-links

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display the parameters and the current state of OSPF virtual links:

```
fwsm/context_name(config)# show ip ospf virtual-links
```

Related Commands

clear ip ospf
ospf (interface submode)
route-map
router ospf
routing interface
show ip ospf border-routers
show ip ospf database
show ip ospf flood-list
show ip ospf interface
show ip ospf neighbor
show ip ospf request-list
show ip ospf retransmission-list
show ip ospf summary-address
show routing

show ip verify

To display the ingress and egress filtering to verify addressing and route integrity statistics, use the **show ip verify** command.

show ip verify [**reverse-path** [**interface** *int_name*]]

show ip verify statistics

Syntax Description

reverse-path	(Optional) Displays the egress filters.
interface *int_name*	(Optional) Name of an interface that you want to display.
statistics	Displays filtering statistics.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display ingress and egress filtering to verify addressing and route integrity statistics:

```
fwsm(config)# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

Related Commands

clear ip verify reverse-path
ip verify reverse-path

show isakmp

To display the Internet Security Association and Key Management Protocol (ISAKMP) identity information, use the **show isakmp** command.

show isakmp sa [**detail**]

show isakmp identity

Syntax Description

sa	Displays all current Internet Key Exchange (IKE) security associations between the FWSM and its peer.
detail	(Optional) Displays detailed ISAKMP identity information.
identity	Displays ISAKMP identity information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Table 2-22 lists the descriptions for the **show isakmp sa detail** command output.

Table 2-22 show isakmp Command Output Field Descriptions

Field	Description
dst	Destination
src	Source
state	Operational state
pending	Pending status
created	When created
Total	Total statistics
Embryonic	Embryonic state
Local	IP address and port of the FWSM on which the command is run (the format is IP_Address:port)
Remote	Peer IP address and port

Table 2-22 show isakmp Command Output Field Descriptions (continued)

Field	Description
Encr	Encryption algorithm
Hash	Hash algorithm
Auth	Authorization method (preshared key, or rsa)
State	State of the connection
Lifetime	Time until the rekey or until expiration and deletion

Examples

This example shows how to display identity information after IKE negotiations were successfully completed between the FWSM and its peer:

```
fwsm/context_name(config)# show isakmp sa
        dst             src          state     pending    created
    16.132.40.2    16.132.30.2    QM_IDLE         0           1
```

This example shows how to display detailed ISAKMP identity information:

```
fwsm/context_name(config)# show isakmp sa detail
Total     : 1
Embryonic : 0
         Local            Remote          Encr  Hash    Auth  State      Lifetime
   192.168.10.2:4500    192.168.10.5:1178 3des  sha     psk  QM_IDLE       117
```

This example shows how to display all IKE security associations between the FWSM and its peer:

```
fwsm/context_name(config)# show isakmp sa
        dst             src          state     pending    created
    16.132.40.2    16.132.30.2    QM_IDLE         0           1
```

show isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy including the default parameters, use th**e show isakmp policy** command.

show isakmp policy

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display output from the **show isakmp policy** command after two IKE policies are configured with priorities 70 and 90:

```
fwsm/context_name(config)# show isakmp policy

Protection suite priority 70
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:       5000 seconds, no volume limit
Protection suite priority 90
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:       10000 seconds, no volume limit
Default protection suite
        encryption algorithm:   DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:       86400 seconds, no volume limit
```

Note Although the output shows “no volume limit” for the lifetimes, you can configure only a time lifetime (such as 86,400 seconds); the volume limit lifetimes are not configurable.

Examples

This example shows sample output from the **show isakmp** and **show isakmp policy** commands for a configuration using Diffie-Hellman group 5 in its ISAKMP policy:

```
fwsm/context_name(config)# show isakmp
isakmp enable outside
isakmp key ******** address 0.0.0.0 netmask 0.0.0.0
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 5
isakmp policy 1 lifetime 86400

fwsm/context_name(config)# show isakmp policy
Protection suite of priority 8
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
```

show local-host

To display the network states of local hosts, use the **show local-host** command.

show local-host [*ip_address*] [**detail**]

Syntax Description

ip_address	(Optional) Local host IP address.
detail	(Optional) Displays the detailed network states of local host information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines

Note Beginning with Release 2.3, using the **show local host** command is not a reliable method for monitoring the rate of SYN attacks.

The **show local-host** command allows you to display the network states of local hosts. Local hosts are any hosts on the same subnet as an internal FWSM interface (not the outside interface).

This command allows you to show the translation and connection slots for the local hosts or stop all traffic on these hosts. This command provides information for hosts that are configured with the **nat 0** command when normal translation and connection states may not apply.

The **show local-host detail** command displays more information about active xlates and connections.

Use the *ip_address* argument to limit the display to a single host.

This command displays the maximum connection value for the UDP protocol. Every time the UPD maximum connection value is not set, the value will be displayed as 0 by default and will not be applied.

In the event of a syn attack (with TCP intercept configured), the **show local-host** command output includes the number of intercepted connections in the usage count. This field typically displays only full open connections.

Examples

This example shows how to display the network states of local hosts:

```
fwsm/context_name(config)# show local-host 10.1.1.15
local host: <10.1.1.15>, conn(s)/limit = 2/0, embryonic(s)/limit = 0/0
   Xlate(s):
       PAT Global 172.16.3.200(1024) Local 10.1.1.15(55812)
       PAT Global 172.16.3.200(1025) Local 10.1.1.15(56836)
       PAT Global 172.16.3.200(1026) Local 10.1.1.15(57092)
       PAT Global 172.16.3.200(1027) Local 10.1.1.15(56324)
       PAT Global 172.16.3.200(1028) Local 10.1.1.15(7104)
   Conn(s):
       TCP out 192.150.49.10:23 in 10.1.1.15:1246 idle 0:00:20 Bytes 449 flags UIO
       TCP out 192.150.49.10:21 in 10.1.1.15:1247 idle 0:00:10 Bytes 359 flags UIO
```

The xlate describes the translation slot information, and the Conn is the connection state information.

This example shows how to display the detailed network state of local host information:

```
fwsm/context_name(config)# show local-host detail
     local host: <10.1.1.15>, conn(s)/limit = 2/0, embryonic(s)/limit = 0/0
         Xlate(s):
             TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024
                       flags ri
             ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0
                       flags ri
             UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024
                       flags ri
         Conn(s):
             TCP outside:192.150.49.10/23 inside:10.1.1.15/1026 flags UIO
             UDP outside:192.150.49.10/31649 inside:10.1.1.15/1028 flags dD
```

Related Commands

clear local-host

show log-adj-changes

To display the syslog message that are sent by the router when an OSPF neighbor goes up or down, use the **show log-adj-changes** subcommand.

show log-adj-changes [**detail**]

Syntax Description

detail	(Optional) Sends a syslog message for each state change, not just when a neighbor goes up or down.

Defaults

Enable

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show log-adj-changes** subcommand is enabled by default, but the **show log-adj-changes** subcommand is only displayed in the OSPF configuration when you specify the **detail** keyword or when you disable the feature.

Examples

This example shows how to display syslog message that are sent by the router when an OSPF neighbor goes up or down:

```
fwsm(config)# show log-adj-changes
```

Related Commands

log-adj-changes (router ospf submode)
router ospf
show ip ospf

show logging

To display the enabled logging options, use the **show logging** command.

show logging message {*syslog_id* | **all**} | **level** | **disabled**}

show logging queue

Syntax Description

message	Displays the syslog messages.
syslog_id	Message number to display.
all	Displays all syslog message IDs.
level	Displays the logging level.
disabled	Displays the suppressed syslog messages.
queue	Displays the syslog message queue.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

If the **logging buffered** command is in use, the **show logging** command allows you to display the current message buffer. The **show logging disabled** command displays suppressed syslog messages.

The **show message disabled** command allows you to list the suppressed messages. All syslog messages are permitted unless explicitly disallowed. You cannot block the "FWSM Startup begin" message, and you cannot block more than one message per command.

If a message is listed in syslog as %FWSM-1-101001, use "101001" as the *syslog_id*.

Note Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Internet Router Firewall Services Module System Message Guide* for message numbers.

The **show logging queue** command allows you to display the following:

- Number of messages that are in the queue
- Highest number of messages recorded that are in the queue
- Number of messages that are discarded because block memory was not available to process them

Examples

This example shows how to display the enabled logging options:

```
fwsm(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

The line of output starting with 305001 shows a translation to a PAT global through global address 209.165.201.5 from a host at 192.168.1.2. The “305001” identifies a syslog message for creating a translation through a PAT global.

This example shows sample output from the **show logging** command with the **logging device-id hostname** command configured on a host named **fwsm-1**:

```
fwsm(config)# logging device-id hostname
fwsm(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: level debugging, 0 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: disabled
Trap logging: disabled
History logging: disabled
Device ID: hostname "fwsm-1"
```

Related Commands

clear logging rate-limit
logging

show logging rate-limit

To display the disallowed messages to the original set, use the **show logging rate-limit** command.

show logging rate-limit

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

After the information is cleared, nothing more displays until the hosts reestablish their connections.

Examples

This example shows how to display the disallowed messages:

```
fwsm/context_name(config)# show logging rate-limit
```

Related Commands

clear logging rate-limit

show mac-address interface

To display the information about the MAC-address on an interface, use the **show mac-address interface** command.

show mac-address interface *ifname*

Syntax Description

ifname	Interface name.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display information abou the MAC-address on an interface:

```
fwsm(config)# show mac-address interface 4
```

Related Commands

clear mac-address-table
mac-address-table aging-time
mac-address-table static

show mac-address-table

To display the information about the MAC-address table, use the **show mac-address-table** command.

show mac-address-table [**static**] [**count**]

Syntax Description

static	(Optional) Displays the static MAC addresses in the bridge table.
count	(Optional) Displays the MAC address table count.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display information about the MAC-address table:

```
fwsm(config)# show mac-address-table
```

Related Commands

clear mac-address-table
mac-address-table aging-time
mac-address-table static

show mac-learn

To display the learned MAC-address information, use the **show mac-learn** command.

show mac-learn

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the learned MAC-address information:

```
fwsm(config)# show mac-learn
```

Related Commands

clear mac-learn

show match

To display the route-map match configuration, use the **show match** command.

show match

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the route-map match configuration:

```
fwsm(config)# show match
```

Related Commands

match (route map submode)
match interface (route map submode)
match ip next-hop (route map submode)
match route-type (route map submode)
route-map

show memory

To display a summary of the maximum physical memory and current free memory that is available to the FWSM operating system, use the **show memory** command.

show memory

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show memory** command allows you to display a summary of the maximum physical memory and current free memory that is available to the FWSM operating system. The memory in the FWSM is allocated as needed.

You can also display the information from the **show memory** command using SNMP.

Examples

This example shows how to display a summary of the maximum physical memory and current free memory that is available to the FWSM:

```
fwsm(config)# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

show mode

To display the current mode for the FWSM, use the **show mode** command.

show mode

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: System and Context

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the current mode for the FWSM:

```
fwsm/context_name(config)# show mode
Firewall mode: multiple
The flash mode is the SAME as the running mode.
```

Related Commands

mode

show mgcp

To display the Media Gateway Control Protocol (MGCP) information, use the **show mgcp** command.

show mgcp {**commands** | **sessions**} [**detail**]

Syntax Description

commands	Displays the number of MGCP commands in the command queue.
sessions	Displays the number of existing MGCP sessions.
detail	(Optional) Displays additional information about each command (or session) in the output.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display MGCP information:

```
fwsm/context_name(config)# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07

fwsm/context_name(config)# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
       Gateway IP      host-pc-2
       Transaction ID  2052
       Endpoint name   aaln/1
       Call ID         9876543210abcdef
       Connection ID
       Media IP        192.168.5.7
       Media port      6058

fwsm/context_name(config)# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
```

```
fwsm/context_name(config)# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
       Gateway IP      host-pc-2
       Call ID         9876543210abcdef
       Connection ID   6789af54c9
       Endpoint name   aaln/1
       Media lcl port  6166
       Media rmt IP    192.168.5.7
       Media rmt port  6058
```

Related Commands

clear mgcp
mgcp

show monitor-interface

To display the information about the monitored interface, use the **show monitor-interface** command.

show monitor-interface

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.
2.3(1)	Support for the Autostate feature was added on the FWSM.

Usage Guidelines

The **show monitor-interface** command allows you to display the interface status for the monitored interfaces in the user context when this command is used in multiple context mode. The interfaces must be configured before you use this command to receive information.

Autostate allows the FWSM to quickly detect the failure of the interfaces connecting the real hosts. To allow autostate support on an FWSM interface, you must enable interface monitoring (see the **monitor-interface** command) on that interface. The switch operating system software informs the FWSM when the first or last physical port has joined or left a VLAN assigned to that FWSM, excluding the FWSM port channel and trunk port to the MSFC.

The FWSM responds to a VLAN down condition by marking the interfaces associated with that VLAN as autostate down. This VLAN is considered as a failed interface for interface monitoring of health status and may cause a failover if the interface policy threshold is met. When you suspend the configuration configuration, two interfaces will no longer synchronize the configuration or replicate commands.

Note When you enable the suspend configuration synchronization, interface monitoring and logical interfaces are disabled.

Examples

This example shows how to display the status of the monitored interfaces (from within the context):

```
primary/contexta(config)# show monitor-interface
        This host: Primary - Active
                Interface outside (88.1.1.2): Normal
                Interface inside (10.6.8.91): Normal
        Other host: Secondary - Standby
                Interface outside (88.1.1.3): Normal
                Interface inside (10.6.8.100): Normal
```

Related Commands

failover interface ip
failover interface-policy
failover lan interface
monitor-interface
show failover
write standby

show mroute

To display the information about the current multicast route table information, use the **show mroute** command.

show mroute [*dst* [*src*]]

Syntax Description

dst	(Optional) Displays multicast route table information that is based on the specified Class D address of the multicast group.
src	(Optional) Displays multicast route table information that is based on the specified IP address of the multicast source.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display information about the current multicast route table:

```
fwsm/context_name(config)# show mroute
```

Related Commands

mtu

show mtu

To display the current maximum transmission unit (MTU) block size, use the **show mtu** command.

show mtu

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show interface** command also shows the MTU value.

Examples

This example shows how to display the current MTU block size:

```
fwsm(config)# show mtu
mtu outside 1500
mtu inside 1500
```

Related Commands

mtu
show interface

show multicast

To display all or per-interface multicast settings, use the **show multicast** command.

show multicast [**interface** *interface_name*]

Syntax Description

interface *interface_name*	(Optional) Displays the per-interface multicast settings.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display all multicast settings:

```
fwsm(config)# show multicast
```

Related Commands

show igmp

show name

To list the **name** commands in the configuration, use the **show name** command.

show name

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to list the **name** command configuration.

```
fwsm(config)# show name
System IP Addresses:
    name 192.168.42.3 fwsm_inside
    name 209.165.201.3 fwsm_outside
```

Related Commands

clear name
name

show nameif

To display the name of an interface, use the **show nameif** command.

show nameif

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the name of an interface:

```
fwsm(config)# show nameif
nameif vlan36 inside security100
nameif vlan22 shared security50
nameif vlan38 dmz security50
nameif vlan10 mgmt security10
nameif vlan37 outside security0
```

Related Commands

nameif

show names

To display the IP address-to-name conversion, use the **show names** command.

show names

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example show how to display the IP address-to-name conversion:

```
fwsm/context_name(config)# show names
System IP Addresses:
    name 192.168.42.3 fwsm_inside
    name 209.165.201.3 fwsm_outside
```

Related Commands

clear name
name
names
show name

show nat

To display a pool of global IP addresses that are associated with a network, use the **show nat** command.

show nat

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines

This command displays the maximum connection value for the UDP protocol. Every time the UPD maximum connection value is not set, the value will be displayed as 0 by default and will not be applied.

Note In transparent mode, only NAT ID 0 is valid.

Examples

This example shows how to display a pool of global IP addresses that are associated with a network:

```
fwsm/context_name(config)# show nat
nat (inside) 1001 36.7.2.0 255.255.255.224 0 0
nat (inside) 1001 36.7.2.32 255.255.255.224 0 0
nat (inside) 1001 36.7.2.64 255.255.255.224 0 0
nat (inside) 1002 36.7.2.96 255.255.255.224 0 0
nat (inside) 1002 36.7.2.128 255.255.255.224 0 0
nat (inside) 1002 36.7.2.160 255.255.255.224 0 0
nat (inside) 1003 36.7.2.192 255.255.255.224 0 0
nat (inside) 1003 36.7.2.224 255.255.255.224 0 0
```

Related Commands

clear nat
nat

show network

To display the interfaces on which the OSPF protocol runs and the area ID for those interfaces, use the **show network** subcommand.

show network *prefix ip_address netmask* **area** *area_id*

Syntax Description

prefix	IP address.
ip_address	Router ID in IP address format.
netmask	IP address mask or IP subnet mask used for a summary route.
area *area_id*	Specifies the area to be configured as a regular OSPF area.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the interfaces on which the OSPF protocol runs:

```
fwsm/context_name(config)# show network area
```

Related Commands

object-group

show nic

To display the status of the internal network interface cards (NICs), use the **show nic** command

show nic

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the status of the internal NICs:

```
fwsm(config)# show nic
interface gb-ethernet0 is up, line protocol is up
  Hardware is i82543 rev02 gigabit ethernet, address is 000b.5f0d.3700
 PCI details are - Bus:0, Dev:0, Func:0
  MTU 1500 bytes, BW 1 Gbit full duplex
        502 packets input, 51236 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        18375 packets output, 1854756 bytes, 0 underruns
        input queue (curr/max blocks): hardware (255/255) software (0/0)
        output queue (curr/max blocks): hardware (0/2) software (0/0)
interface gb-ethernet1 is up, line protocol is up
  Hardware is i82543 rev02 gigabit ethernet, address is 000b.5f0d.3700
 PCI details are - Bus:0, Dev:0, Func:0
  MTU 16000 bytes, BW 1 Gbit full duplex
        12256 packets input, 1424408 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        4 packets output, 280 bytes, 0 underruns
        input queue (curr/max blocks): hardware (255/255) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/0)
```

show object-group

To remove all the **object** commands from the configuration, use the **show object-group** command.

show object-group [**protocol** | **service** | **icmp-type** | **network**]

show object-group id *obj_grp_id*

Syntax Description

protocol	(Optional) Defines a group of protocols such as TCP and UDP.
service	(Optional) Defines a group of TCP/UDP port specifications such as “eq smtp” and “range 2000 2010.”
icmp-type	(Optional) Defines a group of ICMP types such as echo and echo-reply.
network	(Optional) Defines a group of hosts or subnet IP addresses.
obj_grp_id	Name of a previously defined object group.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Table 2-23 lists the descriptions for the **show object-group** commands and their accompanying configuration commands.

Table 2-23 Command Description

Command	Further Configuration
show object-group protocol	After entering this command, add the protocol objects to the protocol group with the **protocol-object** and the **group-object** subcommand.
show object-group service	After entering this command, add the port objects to the service group with the **port-object** and the **group-object** subcommand.
object-group icmp-type	After entering this command, add the ICMP objects to the ICMP type group with the **icmp-object** and the **group-object** subcommand.
object-group network	After entering this command, add the network objects to the network group with the **network-object** and the **group-object** subcommand. To group object groups together, they must be the same type. For example, you can group two or more network object groups together, but you cannot group a protocol group and a network group together.

Examples

This example shows how to remove all the **object** commands from the configuration:

```
fwsm(config)# show object-group
```

Related Commands

clear object-group
object-group

show pager

To display the lines that are configured for screen paging, use the **show pager** command.

show pager

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the lines that are configured for screen paging:

```
fwsm(config)# show pager
pager lines 30
```

Related Commands

clear pager
pager

show password/passwd

To display the Telnet password, use the **show password** command.

show {**password** | **passwd**}

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **passwd** keyword is an accepted shortened form of **password**.

Examples

This example shows how to display the Telnet password:

```
fwsm/context_name(config)# show password
passwd 2KFQnbNIdI.2KYOU encrypted
```

Related Commands

clear password
password/passwd

show pdm

To display the device manager buffer information, use the **show pdm** command.

show pdm history [**view** {**all** | **12h** | **5d** | **60m** | **10m**}] [**snapshot**] [**feature** {**all** | **blocks** | **cpu** | **failover** | **ids** | **interface** *interface_name* | **memory** | **perfmon** | **xlates**}] [**pdmclient**]

show pdm logging

show pdm sessions

Syntax Description

history	Displays the contents of the FDM history buffer.
view all	(Optional) Displays the history for all features.
view 12h | 5d | 60m | 10m | all	(Optional) Specifies the FDM history view to display: 12 hours (**12h**), 5 days (**5d**), 60 minutes (**60m**), 10 minutes (**10m**), or **all** history contents in the FDM history buffer.
snapshot	(Optional) Displays only the last FDM history data point.
feature	(Optional) Displays the history for a single feature; if not specified, the history for all features is displayed.
all	(Optional) Displays the history for all features.
blocks	(Optional) Displays the buffer blocks.
cpu	(Optional) Displays the history for CPU usage; this output is similar to output of the **show cpu** command.
failover	(Optional) Displays the history for failover.
ids	(Optional) Displays the history for the Intrusion Detection System Module (IDSM).
interface *interface_name*	(Optional) Specifies the interface name on which the PDM resides.
memory	(Optional) Displays the history for memory.
perfmon	(Optional) Displays the history for performance.
xlates	(Optional) Displays the history for translation slot information.
pdmclient	(Optional) Displays the FDM history in FDM-display format.
logging	Displays the contents of the FDM logging buffer (located within the FDM).
sessions	Displays the FDM session ID number.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The PDM syslog messages are stored separately from the FWSM syslog messages. The **clear pdm logging** command clears the PDM log without disabling PDM logging.

The **show pdm sessions** command is accessible through the FWSM command-line interface (CLI). The **show pdm sessions** command allows you to display all the active PDM sessions that are connected to the FWSM by a unique se*ssion_id*, beginning with session number 0.

Examples

This example shows how to display the contents of the PDM history buffer:

```
fwsm(config)# show pdm history view 10m snapshot pdmclient
INTERFACE|outside|up|IBC|0|OBC|1088|IPC|0|OPC|0|IBR|17|OBR|0|IPR|0|OPR|0|IERR|1|NB|0|RB|0|
RNT|0|GNT|0|CRC|0|FRM|0|OR|0|UR|0|OERR|0|COLL|0|LCOLL|0|RST|0|DEF|0|LCR|0:FWSMoutsideINTER
FACE:METRIC_HISTORY|SNAP|IBR|VIEW|10|1952|METRIC_HISTORY|SNAP|OBR|VIEW|10|64|METRIC_HISTOR
Y|SNAP|IPR|VIEW|10|17|METRIC_HISTORY|SNAP|OPR|VIEW|10|1|METRIC_HISTORY|SNAP|IERR|VIEW|10|0
|METRIC_HISTORY|SNAP|OERR|VIEW|10|0|:FWSMinsideINTERFACE:METRIC_HISTORY|SNAP|IBR|VIEW|10|0
|METRIC_HISTORY|SNAP|OBR|VIEW|10|64|METRIC_HISTORY|SNAP|IPR|VIEW|10|0|METRIC_HISTORY|SNAP|
OPR|VIEW|10|1|METRIC_HISTORY|SNAP|IERR|VIEW|10|0|METRIC_HISTORY|SNAP|OERR|VIEW|10|0|:FWSMS
YS:METRIC_HISTORY|SNAP|MEM|VIEW|10|52662272|METRIC_HISTORY|SNAP|BLK4|VIEW|10|1600|METRIC_H
ISTORY|SNAP|BLK80|VIEW|10|400|METRIC_HISTORY|SNAP|BLK256|VIEW|10|998|METRIC_HISTORY|SNAP|B
LK1550|VIEW|10|676|METRIC_HISTORY|SNAP|XLATES|VIEW|10|0|METRIC_HISTORY|SNAP|CONNS|VIEW|10|
0|METRIC_HISTORY|SNAP|TCPCONNS|VIEW|10|0|METRIC_HISTORY|SNAP|UDPCONNS|VIEW|10|0|METRIC_HIS
TORY|SNAP|URLS|VIEW|10|0|METRIC_HISTORY|SNAP|WEBSNS|VIEW|10|0|METRIC_HISTORY|SNAP|TCPFIXUP
S|VIEW|10|0|METRIC_HISTORY|SNAP|TCPINTERCEPTS|VIEW|10|0|METRIC_HISTORY|SNAP|HTTPFIXUPS|VIE
W|10|0|METRIC_HISTORY|SNAP|FTPFIXUPS|VIEW|10|0|METRIC_HISTORY|SNAP|AAAAUTHENUPS|VIEW|10|0|
METRIC_HISTORY|SNAP|AAAAUTHORUPS|VIEW|10|0|METRIC_HISTORY|SNAP|AAAACCOUNTS|VIEW|10|0|
```

This example shows how to report the data that is formatted for the FWSM CLI:

```
fwsm(config)# pdm history enable
fwsm(config)# show pdm history view 10m snapshot
Available 4 byte Blocks:  [  10s] : 1600
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 400
.
.
.
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
PPTP Sessions:  [  10s] : 0
PPTP Tunnels:  [  10s] : 0
```

Related Commands

clear pdm
pdm

show perfmon

To display information about the FWSM performance, use the **show perfmon** command.

show perfmon

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command output does not display in a Telnet console session.

The **perfmon** command allows you to monitor the FWSM's performance. The **show perfmon** command allows you to display the information immediately.

Examples

This example shows how to display information about the FWSM performance:

```
fwsm/context_name(config)# show perfmon
Context: admin
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept    322779/s     322779/s
```

Related Commands

perfmon

show privilege

To display the privileges for a command or a set of commands, use the **show privilege** command.

show privilege [**all** | **command** *command* | **level** *level*]

Syntax Description

all	(Optional) Displays the privilege level for all commands.
command *command*	(Optional) Displays the privilege level for a specific command.
level *level*	(Optional) Displays the commands that are configured with the specified level; valid values are from 0 to 15.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: System

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the privileges for level 0 commands:

```
fwsm(config)# show privilege level 0
privilege show level 0 command checksum
privilege show level 0 command curpriv
privilege configure level 0 mode enable command enable
privilege show level 0 command history
privilege configure level 0 command login
privilege configure level 0 command logout
privilege show level 0 command pager
privilege clear level 0 command pager
privilege configure level 0 command pager
privilege configure level 0 command quit
privilege show level 0 command version
```

Related Commands

clear privilege
privilege

show processes

To display a list of the processes that are running on the FWSM, use the **show processes** command.

show processes

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show processes** command allows you to display a list of the processes that are running on the FWSM.

Processes are lightweight threads requiring only a few instructions. In the listing, PC is the program counter, SP is the stack pointer, STATE is the address of a thread queue, Runtime is the number of milliseconds that the thread has been running, SBASE is the stack base address, Stack is the current number of bytes that are used and the total size of the stack, and Process lists the thread's function.

Examples

This example shows how to display a list of processes that are running on the FWSM:

```
fwsm(config)# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->
```

show redistribute

To display the redistribution between OSPF processes according to the parameters specified, use the **show redistribute** command.

show redistribute {**static | connected**} [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

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

Syntax Description

static	(Optional) Specifies the static connections.
connected	(Optional) Specifies the operating connections.
metric *metric_value*	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type *metric_type*	(Optional) Specifies the OSPF metric type; valid values are **type-1**, **type-2**, **internal**, or **external**.
route-map *map_name*	(Optional) Specifies the name of the route map to apply.
tag *tag_value*	(Optional) Specifies the value to match for controlling redistribution with route maps.
subnets	(Optional) Specifies the redistributing routes into OSPF and scopes the redistribution for the specified protocol.
ospf *pid*	Specifies an internally used identification parameter for an OSPF routing process; valid values are from 1 to 65535.
match	(Optional) Specifies the conditions for redistributing routes from one routing protocol into another.
internal *type*	(Optional) Specifies the OSPF metric routes that are internal to a specified autonomous system; valid values are either type 1 or 2.
external *type*	(Optional) Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are either type 1 or 2.
nssa-external *type*	(Optional) Specifies the OSPF metric type for routes that are external to a not-so-stubby area (NSSA); valid values are either type 1 or 2.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

You assign the *pid* locally on the FWSM; it can be from 1 to 65535. You must assign a unique value for each OSPF routing process.

Examples

This example shows how to display the redistribution of processes across OSPF:

```
fwsm(config)# show redistribute
```

Related Commands

redistribute (OSPF submode)
router ospf
show ip ospf

show resource acl-partition

To display partition ACL memory information, use the **show resource acl-partition** command.

show resource acl-partition *context-name*

Syntax Description

context-name	Context.

Defaults

Twelve ACL memory partitions.

Command Modes

Security Context Mode: multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.3(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

This command display the details about all existing partitions. For each partition, the mode (non-exclusive or exclusive) and a list of associated contexts are displayed.

Examples

This example shows how to display partition and ACL memory information:

```
fwsm(config)# show resource acl-partition context!A
```

Related Commands

resource acl-partition

show resource allocation

To display a list of system resource allocations, use the **show resource allocation** command.

show resource allocation [**detail**]

Syntax Description

detail	(Optional) Displays resource allocation details.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show resource allocation** command allows you to display a list of system resource allocations.

Processes are lightweight threads requiring only a few instructions. In the listing, PC is the program counter, SP is the stack pointer, STATE is the address of a thread queue, Runtime is the number of milliseconds that the thread has been running, SBASE is the stack base address, Stack is the current number of bytes that are used and the total size of the stack, and Process lists the thread's function.

Examples

This example shows the total allocation of each resource as an absolute value and as a percentage of the available system resources:

```
fwsm# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           35.00%
 Fixups [rate]              35000           35.00%
 Syslogs [rate]             10500           35.00%
 Conns                     305000           30.50%
 Hosts                      78842           30.07%
 IPsec                          7           35.00%
 SSH                           35           35.00%
 Telnet                        35           35.00%
 Xlates                     91749           34.99%
 All                    unlimited
```

Table 2-24 shows each field description.

Table 2-24 show resource allocation Fields

Field	Description
Resource	Name of the resource that you can limit.
Total	Total amount of the resource that is allocated across all contexts. The amount is an absolute number of concurrent instances or instances per second. If you specified a percentage in the class definition, the FWSM converts the percentage to an absolute number for this display.
% of Avail	The percentage of the total system resources that is allocated across all contexts.

This example shows the **detail** option:

```
fwsm# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     20.00%
                 silver             1      CA      17000      17000     10.00%
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     30.00%

Fixups [rate]    default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     10.00%
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     10.00%

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     20.00%
                 silver             1      CA       3000       3000     10.00%
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     30.00%

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      9.99%
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      9.99%

IPSec            default          all       C          5
                 gold               1       D          5          5     50.00%
                 silver             1      CA          1          1     10.00%
                 bronze             0      CA  unlimited
                 All Contexts:      3                            11    110.00%

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                            20     20.00%
```

```
Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                             20     20.00%

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     10.00%
                 bronze             0      CA      11520
                 All Contexts:      3                          23040     10.00%
mac-addresses    default          all       C      65535
                 gold               1       D      65535      65535    100.00%
                 silver             1      CA       6553       6553      9.99%
                 bronze             0      CA       3276
                 All Contexts:      3                         137623    209.99%
```

Table 2-25 shows each field description.

Table 2-25 show resource allocation detail Fields

Field	Description
Resource	Name of the resource that you can limit.
Class	Name of each class, including the default class. All contexts field shows the total values across all classes.
Mmbrs	Number of contexts assigned to each class.
Origin	Origin of the resource limit, as follows: • A—You set this limit with the **all** option, instead of as an individual resource. • C—This limit is derived from the member class. • D—This limit was not defined in the member class, but was derived from the default class. For a context assigned to the default class, the value will be “C” instead of “D.” FWSM can combine “A” with “C” or “D.”
Limit	Limit of the resource per context, as an absolute number. If you specified a percentage in the class definition, the FWSM converts the percentage to an absolute number for this display.
Total	Total amount of the resource that is allocated across all contexts in the class. The amount is an absolute number of concurrent instances or instances per second. If the resource is unlimited, this display is blank.
% of Avail	Percentage of the total system resources that is allocated across all contexts in the class. If the resource is unlimited, this display is blank.

Related Commands

clear resource usage
show resource types
show resource usage

show resource types

To display a list of system resource types, use the **show resource types** command.

show resource types

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display a list of system resource types:

```
fwsm# show resource types
Rate limited resource types:
  Conns           Connections/sec
  Fixups          Fixups/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  IPsec           IPsec Mgmt Tunnels
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  All             All Resources
```

Related Commands

clear resource usage
show resource allocation
show resource usage

show resource usage

To display a list of system resource usage, use the **show resource usage** command.

show resource usage [**context** *context_name* | **top** n | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

Syntax Description

context	(Optional) Specifies the context.
context_name	(Optional) Name of the context.
top *n*	(Optional) Specifies a number of resources.
all	(Optional) Specifies all resources.
summary	(Optional) Specifies a summary of resources.
system	(Optional) Specifies the system resources.
resource	(Optional) Specifies a specific resource.
rate	(Optional) Specifies a resource rate.
resource_name	(Optional) Resource name.
all	(Optional) Specifies all resources.
detail	(Optional) Specifies detail.
counter	(Optional) Specifies a specific resource counter.
counter_name	(Optional) Specifies the counter name.
count_threshold	(Optional) Specifies the counter threshold.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.
2.3(1)	Support for sync cookies was introduced on the FWSM.

Examples

This example shows how to display a list of system resource usage:

The following sample display shows the resource usage for all contexts and all resources:

```
fwsm# show resource usage summary
Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
```

```
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Fixups [rate]             270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = All contexts are unlimited; system limit is shown.
```

This example shows the amount of resources being used by TCP intercept for individual contexts (sample text in italics shows the TCP intercept information):

```
FWSM(config)# show resource usage detail
Resource              Current         Peak      Limit        Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercept-rate     328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1        N/A             0 admin
console-access-rul          2            2        N/A             0 admin
fixup-rules                14           15        N/A             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2        N/A             0 c1
console-access-rul          2            2        N/A             0 c1
fixup-rules                14           15        N/A             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

This example shows the resources being used by TCP intercept for the entire system (sample text in :

```
FWSM(config)# show resource usage summary detail
Resource              Current         Peak      Limit         Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels             46           48  unlimited             0 Summary
chunk:dbgtrace              4            4  unlimited             0 Summary
chunk:fixup                45           45  unlimited             0 Summary
chunk:global                1            1  unlimited             0 Summary
chunk:hole                  3            3  unlimited             0 Summary
chunk:ip-users             24           24  unlimited             0 Summary
chunk:udp-ctrl-blk          1            1  unlimited             0 Summary
chunk:list-elem          1059         1059  unlimited             0 Summary
chunk:list-hdr             10           11  unlimited             0 Summary
chunk:nat                   1            1  unlimited             0 Summary
chunk:route                 5            5  unlimited             0 Summary
chunk:static                2            2  unlimited             0 Summary
block:16384               510          885       8192(S)          0 Summary
block:2048                 32           35       1000(S)          0 Summary
tcp-intercept-rate     341306       811579  unlimited             0 Summary
globals                     1            1       1051(S)          0 Summary
np-statics                  6            6       4096(S)          0 Summary
statics                     2            2       2048(S)          0 Summary
nats                        1            1       2048(S)          0 Summary
ace-rules                   3            3     116448(S)          0 Summary
console-access-rul          4            4       4356(S)          0 Summary
fixup-rules                43           44       8032(S)          0 Summary
S = System:Total exceeds the system limit; the system limit is shown
```

Related Commands

clear resource usage
show resource allocation
show resource types

show rip

To display the information about the Routing Information Protocol (RIP) configuration, use the **show rip** command.

show rip [*interface_name*]

Syntax Description

interface_name	(Optional) Internal or external network interface to display.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display RIP information:

```
fwsm(config)# show rip
rip outside passive
no rip outside default
rip inside passive
no rip inside default
```

Related Commands

clear rip
rip

show rpc-server

To display the information about the remote processor call (RPC) configuration, use the **show rpc-server** command.

show rpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**TCP** | **UDP**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

Syntax Description

ifc_name	Server interface name.
ip_addr	RPC server IP address.
mask	Network mask.
service	Specifies a service.
service_type	RPC service program number as specified in the **rpcinfo** command.
protocol	Specifies the RPC transport protocol.
tcp	(Optional) Specifies the RPC transport protocol.
udp	(Optional) Specifies the RPC transport protocol.
port *port* [- *port*]	Specifies the RPC protocol port range.
port- *port*	(Optional) Specifies the RPC protocol port range.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the RPC service traffic is closed.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The *service_type* is specified in the **rpcinfo** command.

Examples

This example shows how to display informaton about the RPC configuration:

```
fwsm(config)# show rpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout 0:03:00
```

Related Commands

clear rpc-server
rpc-server

show route

To display a default or static route for an interface, use the **show route** command.

show route [*interface_name ip_address netmask gateway_ip*]

Syntax Description

interface_name	(Optional) Internal or external network interface name.
ip_address	(Optional) Internal or external network IP address.
netmask	(Optional) Network mask to apply to *ip_address*.
gateway_ip	(Optional) IP address of the gateway router (the next-hop address for this route).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system or context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display routes:

```
fwsm(config)# show route
C    10.30.10.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    127.0.0.0 255.255.255.0 is directly connected, eobc
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

Related Commands

clear route
route

show route-map

To display the information about the route map configuration, use the **show route-map** command.

show route-map [*map_tag*]

Syntax Description

map_tag	(Optional) Text for the route-map tag.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Multiple route maps may share the same map tag name.

Examples

This example shows how to display a route map for use in OSPF routing:

```
fwsm(config)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
```

Related Commands

route-map

show router

To display information about the router configuration, use the **show router** command.

show router *ip_address*

Syntax Description

ip_address	Router ID in IP address format.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display information about the router configuration:

```
fwsm(config)# show router 123.456.45.10
```

Related Commands

router
router ospf

show router-id

To display the fixed router ID for an OSPF process, use the **show router-id** command.

show router-id *ip_address*

Syntax Description

ip_address	Router ID in IP address format.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Transparent Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Note If the highest-level IP address on the FWSM is a private address, then this address is sent in hello packets and database definitions (DBDs). To prevent this situation, set the **router-id** *ip_address* to a global address.

Examples

This example shows how to display the fixed router ID for an OSPF process:

```
fwsm(config)# show router-id 123.456.78.10
```

Related Commands

router-id
router ospf
show ip ospf

show routing

To display the nondefault interface-specific routing configuration, use the **show routing** command.

show routing [**interface** *interface_name*]

Syntax Description

interface	(Optional) Specifies the interface.
interface_name	(Optional) Name of the interface for which to display the configuration.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Transparent Mode: routed firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The OSPF routing-related **show** commands are available in privileged mode on the FWSM. You do not need to be in an OSPF configuration submode to use the OSPF-related **show** commands.

Examples

This example shows how to display the nondefault interface-specific routing configurations:

```
fwsm/context_name(config)# show routing
routing interface outside
  ospf retransmit-interval 15
routing interface inside
  ospf cost 206

fwsm/context_name(config)# show routing
Type help or '?' for a list of available commands.
2003 Jul 22 12:42:44 %ETHC-5-PORTTOSTP:Port 4/2 joined
bridge port 4/2
```

This example shows how to display the name of the interface:

```
fwsm/context_name(config)# show routing interface outside
routing interface outside
  ospf retransmit-interval 15
```

Related Commands

route-map
router ospf
routing interface

show running-config

To display the configuration that is running on the FWSM, use the **show running-config** command.

show running-config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Transparent Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show running-config** command allows you to display the current running configuration on the FWSM. Use the **running-config** keyword to match the Cisco IOS software command. The **show running-config** command output is the same as the preexisting FWSM **write terminal** command.

You can use the **running-config** keyword only in the **show running-config** command. You cannot use this keyword with **no** or **clear**, or as a standalone command, because the CLI treats it as a nonsupported command. When you enter the **?**, **no ?**, or **clear ?** keywords, a **running-config** keyword is not listed in the command list.

Note The device manager commands will appear in the configuration after you use FDM to connect to or configure your FWSM.

Examples

This example show how to display the configuration that is running on the FWSM:

```
fwsm/context_name(config)# show running-config
: Saved
:
FWSM Version 2.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname fwsmdoc515
domain-name cisco.com
fixup protocol ftp 21
```

```
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list inside_outbound_nat0_acl permit ip 10.1.3.0 255.255.255.0 10.1.2.0
access-list inside_outbound_nat0_acl permit ip any any
access-list outside_cryptomap_20 permit ip 10.1.3.0 255.255.255.0 10.1.2.0 255.
access-list outside_cryptomap_40 permit ip any any
access-list 101 permit ip any any
pager lines 24
logging on
interface ethernet0 10baset
interface ethernet1 100full
interface ethernet2 100full shutdown
icmp permit any outside
icmp permit any inside
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.23.59.230 255.255.0.0 pppoe
ip address inside 10.1.3.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.0
multicast interface inside
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm location 10.1.2.1 255.255.255.255 outside
pdm location 10.1.2.0 255.255.255.0 outside
pdm logging alerts 100
pdm history enable
arp timeout 14400
global (inside) 6 192.168.1.2-192.168.1.3
global (inside) 3 192.168.4.1
nat (inside) 0 access-list inside_outbound_nat0_acl
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 172.23.59.225 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
```

```
crypto map outside_map 20 set peer 172.23.59.231
crypto map outside_map 20 set transform-set ESP-DES-SHA
crypto map outside_map 40 ipsec-isakmp
crypto map outside_map 40 match address outside_cryptomap_40
crypto map outside_map 40 set peer 123.5.5.5
isakmp key ******** address 172.23.59.231 netmask 255.255.255.255 no-xauth no-c
isakmp peer fqdn no-xauth no-config-mode
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
isakmp policy 40 authentication rsa-sig
isakmp policy 40 encryption 3des
isakmp policy 40 hash sha
isakmp policy 40 group 2
isakmp policy 40 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 10
dhcprelay timeout 60
terminal width 80
Cryptochecksum:4d600490f46b5d335c0fbf2eda0015a2
: end
```

Related Commands

configure

show same-security-traffic

To enable the same-security interface communication, use the **show same-security-traffic** command. To disable the same-security interfaces, use the **no** form of this command.

[**no**] **show same-security-traffic**

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to enable the same-security interface communication:

```
fwsm/context_name(config)# show same-security-traffic
same-security-traffic permit inter-interface
```

Related Commands

clear same-security-traffic
same-security-traffic

show service

To display the system services, use the **show service** command.

show service

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This command shows how to display the system services:

```
fwsm/context_name(config)# show service
service resetinbound
```

Related Commands

clear service
service

show serial

To display the system serial number and licensed services, use the **show serial** command.

show serial

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the system serial number and licensed services:

```
fwsm(config)# show serial
FWSM Firewall Version 2.2(0)141
c6000-fwm-2-1-0-141  #126: Wed Jun 18 16:31:27 MDT 2003
msgreene@boulder-view3:/users/msgreene/projects/firecat/mainline/XFWSM/obj
fwsm up 2 hours 37 mins
Hardware:   WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash  ?V1.01   SMART ATA FLASH DISK @ 0xc321, 20MB
0: gb-ethernet0: irq 5
1: gb-ethernet1: irq 7
2: ethernet0: irq 11
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 100 (per security context)
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Throughput:         Unlimited
ISAKMP peers:       Unlimited
Security Contexts:  2
This machine has an Unrestricted (UR) license.
Serial Number: SAD0649034U
Configuration last modified by enable_15 at 13:56:05 Jul 22 2003
```

Related Commands

uptime

show session

To display an internal AccessPro router console, use the **show session** command.

show session

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to access an internal AccessPro router console:

```
fwsm(config)# show session
Session is disabled
```

Related Commands

set (route map submode)

show set

To display information about the system service setup, use the **show set** command.

show set

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display information about the system service setup:

```
fwsm(config)# show set
service resetinbound
```

Related Commands

set metric (route map submode)
set metric-type (route map submode)

show shun

To display shun information, use the **show shun** command.

show shun [*src_ip* | *statistics*]

Syntax Description

src_ip	(Optional) Address of the attacking host.
statistics	(Optional) Interface counters only.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display shun information:

```
fwsm/context_name(config)# show shun
```

Related Commands

clear shun
shun

show snmp-server

To display information about the SNMP server configuration, use the **show snmp-server** command.

show snmp-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display information about the SNMP server configuration:

```
fwsm/context_name(config)# show snmp-server
snmp-server host perimeter 10.1.2.42
snmp-server location Building 42, Sector 54
snmp-server contact Sherlock Holmes
snmp-server community wallawallabingbang
```

Related Commands

clear snmp-server
snmp-server

show ssh

To list all active Secure Shell (SSH) sessions on the FWSM, use the **show ssh** command.

show ssh sessions [*client_ip*]

show ssh timeout

Syntax Description

sessions	Displays all active SSH sessions on the FWSM.
ip_address	(Optional) IP address of the host or network that is authorized to initiate an SSH connection to the FWSM.
timeout	Specifies the SSH timeout.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The Session ID is a unique number that identifies an SSH session. The Client IP is the IP address of the system running an SSH client. The Version lists the protocol version number that the SSH client supports. The Encryption column lists the type of encryption that the SSH client is using. The State column lists the progress that the client is making as it interacts with the FWSM. The Username column lists the login username that has been authenticated for the session. The "FWSM" username appears when non-AAA authentication is used.

Table 2-26 lists the SSH states that appear in the State column:

Table 2-26 SSH States

Number	SSH State
0	SSH_CLOSED
1	SSH_OPEN
2	SSH_VERSION_OK
3	SSH_SESSION_KEY_RECEIVED
4	SSH_KEYS_EXCHANGED
5	SSH_AUTHENTICATED

Table 2-26 SSH States (continued)

Number	SSH State
6	SSH_SESSION_OPEN
7	SSH_TERMINATE
8	SSH_SESSION_DISCONNECTING
9	SSH_SESSION_DISCONNECTED
10	SSH_SESSION_CLOSED

Examples

This example shows how to list all active SSH sessions on the FWSM:

```
fwsm/context_name(config)# show ssh sessions
Session ID      Client IP       Version Encryption      State   Username
    0           172.16.25.15    1.5     3DES            4       -
    1           172.16.38.112   1.5     DES             6       FWSM
    2           172.16.25.11    1.5     3DES            4       -
```

Related Commands

clear ssh
ssh

show startup-config

To display information about the FWSM startup configuration, use the **show start-config** command.

show startup-config

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show startup-config** command allows you to display the startup configuration of the FWSM. The **startup-config** keyword is used to match the Cisco IOS software command. The **show startup-config** command output is the same as the preexisting FWSM **show configure** command. The **show startup-config** command is not needed for FDM but is provided for compatibility with Cisco IOS software.

You can use the **startup-config** keyword only in the **show startup-config** command. You cannot use the keyword with the **no** or **clear**, or as a standalone command. Because the CLI treats it as a nonsupported command, when you enter the **?**, **no ?**, or **clear ?** keywords, the **startup-config** keyword is not listed in the command list.

Examples

This example shows how to display the FWSM startup configuration:

```
fwsm/context_name(config)# show startup-config
: Saved
: Written by enable_15 at 17:14:09.092 UTC Tue Apr 9 2002
FWSM Version 2.2(0)227
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname fwsmdoc515
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
```

```
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list inside_outbound_nat0_acl permit ip 10.1.3.0 255.255.255.0 10.1.2.0
access-list inside_outbound_nat0_acl permit ip any any
access-list outside_cryptomap_20 permit ip 10.1.3.0 255.255.255.0 10.1.2.0 255.
access-list outside_cryptomap_40 permit ip any any
access-list 101 permit ip any any
pager lines 24
logging on
interface ethernet0 10baset
interface ethernet1 100full
interface ethernet2 100full shutdown
icmp permit any outside
icmp permit any inside
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.23.59.230 255.255.0.0 pppoe
ip address inside 10.1.3.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.0
multicast interface inside
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 0.0.0.0
failover ip address inside 0.0.0.0
failover ip address intf2 0.0.0.0
pdm location 10.1.2.1 255.255.255.255 outside
pdm location 10.1.2.0 255.255.255.0 outside
pdm logging alerts 100
pdm history enable
arp timeout 14400
global (inside) 6 192.168.1.2-192.168.1.3
global (inside) 3 192.168.4.1
nat (inside) 0 access-list inside_outbound_nat0_acl
access-group 101 in interface outside
route outside 0.0.0.0 0.0.0.0 172.23.59.225 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00 s0
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
crypto ipsec transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto map outside_map 20 ipsec-isakmp
crypto map outside_map 20 match address outside_cryptomap_20
crypto map outside_map 20 set peer 172.23.59.231
crypto map outside_map 20 set transform-set ESP-DES-SHA
```

```
crypto map outside_map 40 ipsec-isakmp
crypto map outside_map 40 match address outside_cryptomap_40
crypto map outside_map 40 set peer 123.5.5.5
isakmp key ******** address 172.23.59.231 netmask 255.255.255.255 no-xauth no-c
isakmp peer fqdn no-xauth no-config-mode
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 86400
isakmp policy 40 authentication rsa-sig
isakmp policy 40 encryption 3des
isakmp policy 40 hash sha
isakmp policy 40 group 2
isakmp policy 40 lifetime 86400
telnet timeout 5
ssh timeout 5
```

show static

To display all **static** commands, use the **show static** command.

show static

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines

This command displays the maximum connections value for the UDP protocol. Every time the UPD maximum connections value is not set, the value is displayed as 0 by default and is not applied.

Examples

This example shows how to display all static commands:

```
fwsm/context_name(config)# show static
static (inside,outside) 37.7.1.21 36.7.1.21 netmask 255.255.255.255 255 0
```

Related Commands

clear static
static

show summary-address

To display the aggregate addresses for an OSPF process, use the **show summary-address** command.

show summary-address *addr netmask* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

addr	Value of the summary address that is designated for a range of addresses.
netmask	IP address mask or IP subnet mask that is used for a summary route.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise.
tag *tag_value*	(Optional) Value to match (for controlling redistribution with route maps).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The type 3 summary link-state advertisement (LSA) is suppressed, and the component networks remain hidden from other networks.

In the **summary-address** command, entering the **not-advertise** command suppresses the routes that match the specified prefix or mask pair.

Examples

This example shows how to display the aggregate addresses for OSPF:

```
fwsm/context_name(config)# show summary-address
```

Related Commands

summary-address

show sysopt

To display all the **sysopt** commands from the configuration, use the **show sysopt** command.

show sysopt

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display all **sysopt** commands in the configuration:

```
fwsm/context_name(config)# show sysopt
no sysopt security fragguard
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
sysopt connection zombie timeout 30
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt connection permit-ipsec
no sysopt ipsec pl-compatible
no sysopt route dnat
```

Related Commands

clear sysopt
sysopt

show tech-support

To display the information that is used for diagnosis by technical support analysts, use the **show tech-support** command.

show tech-support [*url*] [**no-config**] [**detail**]

Syntax Description

url	(Optional) URL to which information is sent.
no-config	(Optional) Excludes the output of the running configuration.
detail	(Optional) Lists detailed information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show tech-suppor**t command allows you to list information that technical support analysts need to help you diagnose FWSM problems. This command combines the output from the **show** commands that provide the most information to a technical support analyst.

Examples

This example shows how to display information that is used for technical support analysis:

```
fwsm(config)# show tech-support no-config

Cisco FWSM Firewall Version 2.2(1)
Cisco Device Manager Version 2.2(1)

Compiled on Fri 15-Nov-02 14:35 by root

FWSM up 2 days 8 hours

Hardware:   FWSM, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
```

```
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This FWSM has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:14.911 UTC Sun Nov 17 2002

------------------ show memory ------------------

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
```

```
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 FWSM Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 FWSM/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 FWSM/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 FWSM/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 FWSM/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 FWSM/intf2
H*  0011d7f7 0009ff2c 0053e5b0        780 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  121094970 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3832/4096 tcp_thread/0
```

```
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205213.390 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205213.390 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205215.800 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.800 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

This example shows how to display technical support information that includes the running configuration:

```
fwsm(config)# show tech-support

Cisco FWSM Firewall Version 2.2(1)
Cisco Device Manager Version 2.2(1)

Compiled on Fri 15-Nov-02 14:35 by root

FWSM up 2 days 9 hours

Hardware:   FWSM, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This FWSM has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:39.591 UTC Sun Nov 17 2002

------------------ show memory ------------------

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919
```

```
------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 FWSM Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
```

```
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 FWSM/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 FWSM/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 FWSM/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 FWSM/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 FWSM/intf2
H*  0011d7f7 0009ff2c 0053e5b0        950 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  121109610 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3832/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205238.740 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205238.740 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205242.200 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205242.200 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205242.200 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205242.200 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------
```

```
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s

------------------ show running-config ------------------

: Saved
:
FWSM Version 2.2(1)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname FWSM
domain-name cisco.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
fixup protocol sip udp 5060
names
access-list 101 permit tcp any host 10.1.1.3 eq www
access-list 101 permit tcp any host 10.1.1.3 eq smtp
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
ip address outside 172.23.59.232 255.255.0.0
ip address inside 10.1.1.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
route outside 0.0.0.0 0.0.0.0 172.23.59.225 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 10.1.1.2 255.255.255.255 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
banner exec working...
banner motd Haveagoodday
Cryptochecksum:00000000000000000000000000000000
: end
```

show terminal

To display the console terminal settings, use the **show terminal** command.

show terminal

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display terminal settings:

```
fwsm(config)# show terminal
Width = 511, monitor
```

Related Commands

terminal

show tcpstat

To display the status of the FWSM TCP stack and the TCP connections that are terminated on the FWSM (for debugging), use the **show tcpstat** command.

show tcpstat

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show tcpstat** command allows you to display the status of the TCP stack and TCP connections that are terminated on the FWSM. The TCP statistics displayed are described in Table 2-27.

Table 2-27 TCP Statistics in the show tcpstat Command

Statistic	Description
tcb_cnt	Number of TCP users.
proxy_cnt	Number of TCP proxies. TCP proxies are used by user authorization.
tcp_xmt pkts	Number of packets that were transmitted by the TCP stack.
tcp_rcv good pkts	Number of good packets that were received by the TCP stack.
tcp_rcv drop pkts	Number of received packets that the TCP stack dropped.
tcp bad chksum	Number of received packets that had a bad checksum.
tcp user hash add	Number of TCP users that were added to the hash table.
tcp user hash add dup	Number of times a TCP user was already in the hash table when trying to add a new user.
tcp user srch hash hit	Number of times a TCP user was found in the hash table when searching.
tcp user srch hash miss	Number of times a TCP user was not found in the hash table when searching.

Table 2-27 TCP Statistics in the show tcpstat Command (continued)

Statistic	Description
tcp user hash delete	Number of times that a TCP user was deleted from the hash table.
tcp user hash delete miss	Number of times that a TCP user was not found in the hash table when trying to delete the user.
lip	Local IP address of the TCP user.
fip	Foreign IP address of the TCP user.
lp	Local port of the TCP user.
fp	Foreign port of the TCP user.
st	State (see RFC 793) of the TCP user. The possible values are as follows: 1 CLOSED 2 LISTEN 3 SYN_SENT 4 SYN_RCVD 5 ESTABLISHED 6 FIN_WAIT_1 7 FIN_WAIT_2 8 CLOSE_WAIT 9 CLOSING 10 LAST_ACK 11 TIME_WAIT
rexqlen	Length of the retransmit queue of the TCP user.
inqlen	Length of the input queue of the TCP user.
tw_timer	Value of the time_wait timer (in milliseconds) of the TCP user.
to_timer	Value of the inactivity timeout timer (in milliseconds) of the TCP user.
cl_timer	Value of the close request timer (in milliseconds) of the TCP user.
per_timer	Value of the persist timer (in milliseconds) of the TCP user.
rt_timer	Value of the retransmit timer (in milliseconds) of the TCP user.
tries	Retransmit count of the TCP user.

Examples

This example shows how to display the status of the TCP stack on the FWSM:

```
fwsm(config)# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
```

```
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st
= 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

Related Commands

show conn

show telnet

To display the current list of IP addresses that are authorized to use Telnet connections to the FWSM, use the **show telnet** command.

show telnet [**timeout**]

Syntax Description

timeout	(Optional) Displays the number of minutes that a Telnet session can be idle before being closed by the FWSM.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **no telnet** or **clear telnet** command allows you to remove Telnet access from a previously set IP address. The **clear telnet** command does not affect the **telnet timeout** command duration.

Examples

This example shows how to display the current list of IP addresses that are authorized for use by Telnet connections to the FWSM:

```
fwsm/context_name(config)# show telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

Related Commands

clear telnet
telnet

show tftp-server

To display the **tftp-server** commands in the current configuration, use the **show tftp-server** command.

show tftp-server

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the **tftp-server** commands in the current configuration:

```
fwsm/context_name(config)# show tftp-server
```

Related Commands

clear tftp-server
tftp-server

show timeout

To display the timeout value of the designated protocol, use the **show timeout** command.

show timeout *protocol*

Syntax Description

protocol	(Optional) Protocol to display the timeout value.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the timeout values for the system:

```
fwsm/context_name(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
```

This example shows how to display timeout information for the H323 protocol:

```
fwsm/context_name(config)# show timeout h323
timeout h323 0:05:00
```

Related Commands

clear timeout
timeout

show timers

To display the OSPF process delay timers, use the **show timers** command.

show timers {**spf** *spf_delay spf_holdtime* | **lsa-group-pacing** *seconds*}

Syntax Description

spf *spf_delay*	Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds from 0 to 65535.
spf *spf_holdtime*	Hold time between two consecutive SPF calculations in seconds; valid values are from 0 to 65535.
lsa-group-pacing *seconds*	Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation and the hold time between two consecutive SPF calculations; valid values are from 10 to 1800 seconds.

Defaults

The defaults are as follows:

- *spf_delay* is 5 seconds.
- *spf_holdtime* is 10 seconds.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To configure the delay time between when OSPF receives a topology change and when it starts an SPF calculation and the hold time between two consecutive SPF calculations, use the **show timers spf** *spf_delay spf_holdtime* subcommand.

To change the interval at which the OSPF LSAs are collected into a group and refreshed, checksummed, or aged, use the **show timers lsa-group-pacing** *seconds* subcommand.

Examples

This example shows how to display the OSPF process delay timers:

```
fwsm/context_name(config)# show timers
```

Related Commands

router ospf
show ip ospf
timers

show uauth

To display all the authorization caches for a user, use the **show uauth** command.

clear uauth [*username*]

Syntax Description

username	(Optional) Username that displays the user authentication information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show uauth** command allows you to display one or all currently authenticated users, the host IP to which they are bound, and, if applicable, any cached IP and port authorization information. The **show uauth** command also lists CiscoSecure 2.1 and later idle time and timeout values, which can be set for different user groups.

This command is used with the **timeout** command.

Each user host's IP address has an authorization cache. If the user attempts to access a service that has been cached from the correct host, the FWSM considers it preauthorized and immediately proxies the connection, which means that once a user is authorized to access a website, the authorization server is not contacted for each of the images as they are loaded (if they come from the same IP address). This process significantly increases performance and reduces load on the authorization server.

The cache allows up to 16 address and service pairs for each user host.

The output from the **show uauth** command displays the username that is provided to the authorization server for authentication and authorization, the IP address to which the username is bound, and whether the user is authenticated only or has cached services.

Note When you enable Xauth, an entry is added to the uauth table (as shown by the **show uauth** command) for the IP address that is assigned to the client. When using Xauth with the Easy VPN Remote feature in Network Extension Mode, the IPSec tunnel is created from network to network, so that the users behind the firewall cannot be associated with a single IP address. A uauth entry cannot be created upon completion of Xauth. If AAA authorization or accounting services are required, you can enable the AAA authentication proxy to authenticate users behind the firewall. For more information on AAA authentication proxies, see the **aaa** commands.

Use the **timeout uauth** command to specify how long the cache should be kept after the user connections become idle. Use the **clear uauth** command to delete all authorization caches for all users, which will cause them to reauthenticate the next time that they create a connection.

Examples

This example shows sample output from the **show uauth** command when no users are authenticated and one user authentication is in progress:

```
fwsm(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

This example shows sample output from the **show uauth** command when three users are authenticated and authorized to use services through the FWSM:

```
fwsm(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

Related Commands

aaa authorization
clear uauth
timeout

show uptime

To display the FWSM version and time that the module has been running, use the **show uptime** command.

show uptime

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to configure a route map for OSPF routing:

```
fwsm/context_name(config)# show uptime

FWSM Firewall Version 2.2(0)141

c6000-fwm-2-1-0-141  #126: Wed Jun 18 16:31:27 MDT 2003
msgreene@boulder-view3:/users/msgreene/projects/firecat/mainline/XFWSM/obj

fwsm up 2 hours 34 mins
Configuration last modified by enable_15 at 13:43:59 Jul 22 2003
```

Related Commands

uptime

show url-block

To display the number of packets in the URL-block buffer and the number of packets (if any) that were dropped due to exceeding the buffer limit or retransmission, use the **show url-block** command.

show url-block [**stat**]

Syntax Description

stat	(Optional) Displays the usage statistics for the block buffer usage statistics.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the number of packets in the URL-block buffer and the number of dropped packets that exceeded the buffer limit:

```
fwsm(config)# show url-block
    url-block url-mempool 128
    url-block url-size 4
    url-block block 128

fwsm(config)# show url-block block stat

URL Pending Packet Buffer Stats with max block  128
-----------------------------------------------------
Cumulative number of packets held:              896
Maximum number of packets held (per URL):       3
Current number of packets held (global):        38
Packets dropped due to
       exceeding url-block buffer limit:        7546
       HTTP server retransmission:              10
Number of packets released back to client:      0
```

Related Commands

clear url-block
url-block

show url-cache stat

To display the additional URL cache statistics, including the number of cache lookups and hit rate, use the **show url-cache stat** command.

show url-cache stat

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show url-cache stat** command allows you to display these entries:

- Size—The size of the cache in kilobytes that are set with the **url-cache** *size* keyword and argument.
- Entries—The maximum number of cache entries that are based on the cache size.
- In Use—The current number of entries in the cache.
- Lookups—The number of times that the FWSM has looked for a cache entry.
- Hits—The number of times that the FWSM has found an entry in the cache.

You can display additional information about N2H2 or Websense filtering activity with the **show perfmon** command.

Examples

This example shows how to display additional URL cache statistics:

```
fwsm/context_name(config)# show url-cache stat

URL Filter Cache Stats
----------------------
    Size :     1KB
 Entries :      36
  In Use :      30
 Lookups :      300
    Hits :      290
```

Related Commands

clear url-cache
url-cache

show url-server

To display the URL server information, use the **show url-server** command.

show url-server [**stat**]

Syntax Description

stat	(Optional) Displays the block buffer usage statistics.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show url-server stats** command allows you to display the following information for N2H2 and Websense:

- URL server vendor
- Number of URLs total, allowed, and denied
- Number of HTTPS connections total, allowed, and denied
- Number of TCP connections total, allowed, and denied
- URL server status

Examples

This example shows how to display URL server information:

```
fwsm/context_name(config)# show url-server stat

URL Server Statistics:
----------------------
Vendor websense
HTTPs total/allowed/denied 0/0/0
HTTPSs total/allowed/denied 0/0/0
FTPs total/allowed/denied 0/0/0


URL Server Status:
------------------
172.23.58.103 UP
```

```
URL Packets Send and Recieve Stats:
------------------------------------
Message Send Recieve
STATUS_REQUEST 200 200
LOOKUP_REQUEST 10 10
LOG_REQUEST 20 NA
```

Related Commands

clear url-server
url-server

show username

To display the users that are entered in the local FWSM user authentication database, use the **show username** command.

show username *name*

Syntax Description

name	Name of the specified user.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the users that are entered in the local FWSM user authentication database:

```
fwsm/context_name(config)# show username
```

Related Commands

clear username
username

show version

To display the FWSM software version, hardware configuration, license key, and related uptime data, use the **show version** command.

show version

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: Unprivileged

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show version** command allows you to display the FWSM's software version, operating time since the last reboot, processor type, Flash partition type, interface boards, serial number (BIOS ID), activation key value, license type (R or UR), and time stamp for when the configuration was last modified.

The serial number listed with the **show version** command is for the Flash partition BIOS. This number is different from the serial number on the chassis. When you get a software upgrade, you will need the serial number that appears in the **show version** command, not the chassis number.

Note The uptime value indicates how long a failover set has been running. If one unit stops running, the uptime value will continue to increase as long as the other unit continues to operate.

Examples

This example shows how to display the FWSM software version, hardware configuration, license key, and related uptime information:

```
fwsm(config)# show version

FWSM Firewall Version 2.2(0)197

c6000-fwm-2-1-0-197  #0: Mon Oct 20 01:46:41 MDT 2003
    dalecki@boulder-view1:/auto/bldr-fornax/main/2-1-0-197/Xpix/obj

FWSM up 1 day 23 hours
```

```
Hardware:   WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash  ?V1.01   SMART ATA FLASH DISK @ 0xc321, 20MB

0: gb-ethernet0: irq 5
1: gb-ethernet1: irq 7
2: ethernet0: irq 11

Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 256
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Throughput:         Unlimited
ISAKMP peers:       Unlimited
Security Contexts:  250

This machine has an Unrestricted (UR) license.

Serial Number: SAD070900EU
Configuration last modified by enable_15 at 14:54:58 Oct 23 2003
```

Related Commands

show hw
show serial
show uptime

show virtual

To display the FWSM virtual server settings in the configuration, use the **show virtual** command.

show virtual

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the FWSM virtual server configuration settings:

```
fwsm(config)# show virtual
```

Related Commands

clear virtual
virtual

show vlan

To display the system VLANs, use the **show vlan** command.

show vlan

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display the system VLANs:

```
fwsm(config)# show vlan
10-11, 30, 40, 300
```

show vpngroup

To display the Cisco VPN Client version 3.x (Cisco Unified VPN Client Framework) and Easy VPN Remote devices, use the **show vpngroup** command.

show vpngroup [*group_name*]

Syntax Description

group_name	(Optional) Dynamically generated configuration information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to display VPN device information:

```
fwsm/context_name(config)# show vpngroup
```

Related Commands

clear vpngroup
vpngroup

show who

To display the active Telnet administration sessions on the FWSM, use the **show who** command.

show who [*local_ip*]

Syntax Description

local_ip	(Optional) Internal IP address to limit the listing to one IP address or to a network IP address.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **show who** command allows you to show the FWSM TTY_ID and IP address of each Telnet client that is currently logged into the FWSM. This command is the same as the **who** command.

Examples

This example shows how to display active Telnet administration sessions for the FWSM:

```
fwsm/context_name(config)# show who

0: From 192.168.1.3
1: From 192.168.2.2
```

Related Commands

who

show xlate

To display information about the translation slot, use the **show xlate** command.

show xlate [**global** | **local** *ip1*[**-***ip2*] [**netmask** *mask*]] {**gport** | **lport** *port1* [**-***port2*]}
[**interface** *if1*[**,***if2*]] [**state** *static* [**,portmap**] [**,norandomseq**] [**,identity**]] [**debug**] [**count**]

Syntax Description

global	(Optional) Displays the active translations by global IP address.
local *ip1*	(Optional) Displays the active translations by local IP address.
local -*ip2*	(Optional) Displays the active translations by local IP address for the secondary port.
netmask *mask*	(Optional) Specifies the network mask to qualify the global or local IP addresses.
gport *port*	Displays the active translations by the primary global port specifications. See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names.
lport	Displays the active translations by local port specifications. See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names.
gport -*port*	Displays the active translations by the secondary global port specifications. See the "Specifying Port Values" section in Appendix B, "Port and Protocol Values," for a list of valid port literal names.
interface	(Optional) Displays the active translations by interface.
if1 **,***if2*	(Optional) Interface.
state	(Optional) Displays the active translations by state.
static	(Optional) Static.
,portmap	(Optional) Specifies the port map.
norandomseq	(Optional) Specifies no random sequence.
,identity	(Optional) Specifies the identity.
debug	(Optional) Specifies debugging.
count	(Optional) Specifies the count.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration and privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **clear xlate** command allows you to clear the contents of the translation slots. ("xlate" means translation slot.) The **show xlate** command displays the contents of only the translation slots.

Translation slots can persist after key changes have been made. Always use the **clear xlate** command after adding, changing, or removing the **aaa-server**, **access-list**, **alias**, **global**, **nat**, **route**, or **static** commands in your configuration.

The **show xlate detail** command displays the following information:

- {ICMP|TCP|UDP} PAT from *interface*:*real-address*/*real-port* to *interface*:*mapped-address*/*mapped-port* flags *translation-flags*
- NAT from *interface*:*real-address*/*real-port* to *interface*:*mapped-address*/*mapped-port* flags *translation-flags*

The translation flags are defined in Table 2-28.

Table 2-28 Translation Flags

Flag	Description
s	Static translation slot
d	Dump translation slot on next cleaning cycle
r	Port map translation (Port Address Translation)
n	No randomization of TCP sequence number
o	Outside address translation
i	Inside address translation
D	DNS A RR rewrite
I	Identity translation from **nat 0**

Examples

This example shows how to display the translation slot information with three active Port Address Translations (PATs):

```
fwsm(config)# show xlate
3 in use, 3 most used
PAT Global 192.150.49.1(0) Local 10.1.1.15 ICMP id 340
PAT Global 192.150.49.1(1024) Local 10.1.1.15(1028)
PAT Global 192.150.49.1(1024) Local 10.1.1.15(516)
```

This example shows how to display the translation type and interface information with three active PATs:

```
fwsm(config)# show xlate detail
3 in use, 3 most used
Flags: D - DNS, d - dump, I - identity, i - inside, n - no random,
       o - outside, r - portmap, s - static
TCP PAT from inside:10.1.1.15/1026 to outside:192.150.49.1/1024 flags ri
UDP PAT from inside:10.1.1.15/1028 to outside:192.150.49.1/1024 flags ri
ICMP PAT from inside:10.1.1.15/21505 to outside:192.150.49.1/0 flags ri
```

The first entry is a TCP PAT for host port (10.1.1.15, 1025) on the inside network to host-port (192.150.49.1, 1024) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address port.

The second entry is a UDP PAT for host port (10.1.1.15, 1028) on the inside network to host port (192.150.49.1, 1024) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address port.

The third entry is an ICMP PAT for host-ICMP-id (10.1.1.15, 21505) on the inside network to host-ICMP-id (192.150.49.1, 0) on the outside network. The r flag indicates that the translation is a PAT. The i flag indicates that the translation applies to the inside address ICMP ID.

The inside address fields appear as source addresses on packets traversing from the more secure interface to the less secure interface. They appear as destination addresses on packets traversing from the less secure interface to the more secure interface.

This example shows sample output from two static translations. The first translation has two associated connections (called “nconns”), and the second translation has four associated commands.

```
fwsm(config)# show xlate
Global 209.165.201.10 Local 209.165.201.10 static nconns 1 econns 0
Global 209.165.201.30 Local 209.165.201.30 static nconns 4 econns 0
```

Related Commands

show conn
show uauth
timeout

shun

To enable a dynamic response to an attacking host by preventing new connections and disallowing packets from any existing connection, use the **shun** command. To disable a shun that is based on the *src_ip*, the actual address that is used by the FWSM for shun lookups, use the **no** form of this command.

shun *src_ip* [*dst_ip src_port dest_port* [*protocol*]] *vlan*

Syntax Description

src_ip	Address of the attacking host.
dst_ip	(Optional) Address of the target host.
src_port	(Optional) Source port of the connection causing the shun.
dest_port	(Optional) Destination port of the connection causing the shun.
protocol	(Optional) IP protocol, such as UDP or TCP.
vlan	VLAN.

Defaults

If you use the **shun** command only with the source IP address of the host, then the default is 0.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **shun** command allows you to apply a blocking function to the interface receiving the attack. Packets containing the IP source address of the attacking host are dropped and logged until the blocking function is removed manually or by the Cisco IDS master module. No traffic from the IP source address is allowed to traverse the FWSM. Any remaining connections time out as part of the normal architecture. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you use the **shun** command only with the source IP address of the host, then the default is 0. No further traffic from the offending host is allowed.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the FWSM configuration.

Whenever an interface is removed, all shuns that are attached to that interface are also removed. If you add a new interface or replace the same interface (same name), then you must add that interface to the IDS Sensor if you want the IDS Sensor to monitor that interface.

Examples

This example shows that the offending host (10.1.1.27) makes a connection with the victim (10.2.2.89) with TCP. The connection in the FWSM connection table reads as follows:

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

If you applied the **shun** command in the following way:

```
fwsm/context_name(config)# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

the preceding command deletes the connection from the FWSM connection table and also prevents packets from 10.1.1.27 from going through the FWSM. The offending host can be inside or outside of the FWSM.

Related Commands

clear shun
show shun

shutdown

To shut down the module, use the **shutdown** command. To stop the module shutdown, use the **no** form of this command.

shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Examples

This example shows how to shut down the module:

```
fwsm(config)# shutdown
```

Related Commands

reload

snmp-server

To provide the FWSM event information through SNMP, use the **snmp-server** command. To disable the SNMP commands, use the **no** form of this command.

[**no**] **snmp-server** {**community** *key*} | {**contact** | **location**} *text*} |

[**no**] **snmp-server** {**host** [*interface_name*] *ip_addr* [**trap** | **poll**] [**udp-port** *port*]

[**no**] **snmp-server enable traps** [**all** | *feature* [*trap1 ... trapn*]]

Syntax Description

community *key*	Specifies the password key value at the SNMP management station.
contact *text*	Specifies the name of the contact person or the FWSM system administrator.
location *text*	Specifies the FWSM location.
host	Specifies an IP address of the SNMP management station to which traps should be sent and/or from which the SNMP requests come.
interface_name	(Optional) Interface name where the SNMP management station resides.
ip_addr	IP address of a host to which SNMP traps should be sent and/or from which the SNMP requests come.
trap	(Optional) Specifies that only traps are sent and that this host is not allowed to poll.
poll	(Optional) Specifies that this host is allowed to poll.
udp-port *port*	(Optional) Specifies to override the default SNMP trap port. This keyword and option is only valid when the host may receive traps.
enable traps	Enables sending log messages as SNMP trap notifications.
all	(Optional) Enables or disables traps for all features.
feature	(Optional) Feature for which traps are enabled.
trap1 ... trapn	(Optional) Specifies a trap or range of traps to enable.

Defaults

The defaults is **public** if *key* is not set and both traps and polls are acted upon.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.3(1)	Support for enabling and disabling event logging for individual MIBs was introduced on the FWSM.

Usage Guidelines

The **snmp-server** command allows you to identify the site, management station, community string, and user information.

Note In the **snmp-server community** *key* command, the default value for *key* is **public**. It is important that you specify a (new) value for *key* for security reasons.

Enter the password key in use at the SNMP management station. The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. The FWSM uses the key to determine if the incoming SNMP request is valid. For example, you could designate a site with a community string and then configure the routers, FWSM, and the management station with this same string. The FWSM uses this string and does not respond to requests with an invalid community string.

The *key* is case sensitive and can be up to 32 characters. Spaces are not permitted. The default is **public** if *key* is not set. You must specify a (new) value for *key* for security reasons.

The **contact** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

The **location** *text* is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

You can specify up to 32 SNMP management stations.

Entering the trap command causes only traps to be sent; the host is not allowed to poll.

The **clear snmp-server** and **no snmp-server** commands disable the SNMP commands in the configuration as follows:

```
fwsm/context_name(config)# no snmp-server location
fwsm/context_name(config)# no snmp-server contact
fwsm/context_name(config)# snmp-server community public
fwsm/context_name(config)# no snmp-server enable traps
```

The **snmp-server enable events** command allows you to disable event logging for individual MIB such as the firewall MIB.

Examples

This example shows how to receive SNMP requests from a management station:

```
fwsm/context_name(config)# snmp-server community wallawallabingbang
fwsm/context_name(config)# snmp-server location Building 42, Sector 54
fwsm/context_name(config)# snmp-server contact Sherlock Holmes
fwsm/context_name(config)# snmp-server host perimeter 10.1.2.42
```

Related Commands

clear snmp-server
show snmp-server

ssh

To add SSH access to the FWSM console, set the idle timeout, display the list of active SSH sessions, and terminate an SSH session, use the **ssh** command. To remove the **ssh** commands from the configuration, use the **no** form of this command.

ssh *local_ip mask* [*interface_name*]

ssh timeout *number*

ssh disconnect *session_id*

no ssh {*local_ip* [*mask*] [*interface_name*] | **timeout** | **disconnect**}

Syntax Description

local_ip	IP address of the host or network authorized to initiate an SSH connection to the FWSM.
mask	Network mask for *ip_address*. If you do not specify a *netmask*, the default is 255.255.255.255 regardless of the class of *ip_address*.
interface_name	(Optional) FWSM interface name on which the host or network initiating the SSH connection resides.
timeout *mm*	Specifies the duration in minutes that a session can be idle before being disconnected; valid values are from 1 to 60 minutes.
disconnect *session_id*	Disconnects the specified SSH session by its ID number.

Defaults

The defaults are as follows:

- The **timeout** *mm* is **5** minutes.
- If you do not specify a *netmask*, the default is 255.255.255.255 regardless of the class of *ip_address*.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **ssh** *ip_address* command allows you to specify the host or network that is authorized to initiate an SSH connection to the FWSM.

Note Only DES and 3DES ciphers are supported. If you use another cipher, the connection will be denied.

The **ssh timeout** command allows you to specify the duration in minutes that a session can be idle before being disconnected. The default duration is 5 minutes. Use the **show ssh sessions** command to find the session ID number. Use the **no ssh** command to remove the selected **ssh** commands from the configuration.

Examples

This example shows how to create an RSA key-pair with a modulus size of 1024 bits (recommended for use with Cisco IOS software), set the host name and domain name for the FWSM, generate the RSA key-pair, display the RSA key-pair, and save the RSA key-pair to the Flash partition.

```
fwsm/context_name(config)# hostname cisco-fwsm
fwsm/context_name(config)# domain-name example.com
fwsm/context_name(config)# ca generate rsa key 1024
fwsm/context_name(config)# show ca mypubkey rsa
fwsm/context_name(config)# ca save all
```

This example shows how to start an SSH session so that clients on the outside interface can access the FWSM console remotely over a secure shell:

```
fwsm/context_name(config)# ssh 10.1.1.1 255.255.255.255 outside
fwsm/context_name(config)# ssh timeout 60
```

This example shows how to configure the FWSM to perform user authentication using AAA servers. The protocol is the protocol that is used by the AAA server to perform the authentication. This example uses the TACACS+ authentication protocol:

```
fwsm/context_name(config)# aaa-server ssh123 (inside) host 10.1.1.200 mysecure
fwsm/context_name(config)# aaa-server ssh123 protocol tacacs+
fwsm/context_name(config)# aaa authenticate ssh console ssh123
```

Related Commands

aaa accounting
ca authenticate
clear ssh
domain-name
hostname
password/passwd
show ssh

static

To configure a persistent one-to-one address translation rule by mapping a local IP address to a global IP address, use the **static** command. To restore the default settings, use the **no** form of this command.

[**no**] **static** [*real_ifc*, *mapped_ifc*] {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*]} | {**access-list** *access_list_name*} [**dns**] [**norandomseq**] [[**tcp**] [*max_conns* [*emb_lim*]] [**udp** *udp_max_conns*]

[**no**] **static** [*real_ifc*, *mapped_ifc*] {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip* *real_port* [**netmask** *mask*]} | {**access-list** *access_list_name*} [**dns**] [**norandomseq**] [[**tcp**] [*max_conns* [*emb_lim*]] [**udp** *udp_max_conns*]

Syntax Description

real_ifc	(Optional) Name of the network interface, as specified by the **nameif** command, where the hosts or networks designated by the specified *real_ip* or sources in the access list are accessed.
mapped_ifc	(Optional) Name of the network interface, as specified by the **nameif** command, where the *real_ip* argument or by the source in the access-list are translated into the *mapped_ip* argument.
mapped_ip	Masquerade address of the *real_ip* argument or of the source address in the access-list.
interface	Specifies the address taken from the *mapped_ifc* argument.
real_ip	Address as configured at the actual host.
netmask *mask*	(Optional) Specifies the IP netmask to apply to the specified *real_ip* argument.
access-list	Allows you to identify local traffic for network address translation (NAT) by specifying the local and destination addresses (or ports).
access_list_name	Access list name.
dns	(Optional) Rewrites the local address in DNS replies to the global address.
norandomseq	(Optional) Disables the TCP Initial Sequence Number (ISN) randomization protection.
tcp	(Optional) Specifies that maximum TCP connections and embryonic limits are set for TCP.
max_conns	(Optional) Maximum number of simultaneous TCP connections that each *real_ip* variable host is allowed to use. Idle connections are closed after the time specified by the **timeout conn** command.
emb_lim	(Optional) Maximum number of embryonic connections per host. An embryonic connection is a connection request that has not completed a TCP 3-way handshake between the source and destination.
udp	(Optional) Specifies that a maximum number of UDP connection parameters are configured.
udp_max_conns	(Optional) Used with the **udp** keyword to set the maximum number of simultaneous UDP connections that the *local_ip* hosts are each allowed to use.
tcp	Specifies the TCP static PAT.
udp	Specifies the UDP static PAT.
mapped_ip	Mapped IP address; the mapped IP address and the real IP address must be in the same network.
mapped_port	Masquerade port of the specified *real_port* or of the source port in the access list.

real_port	Port viewed from the actual host.
netmask	(Optional) Specifies the keyword required before specifying the network mask. If you do not enter a mask, then the default mask for the IP address class is used.

Defaults

The defaults are as follows:

- Embryonic is 0.
- **udp** is not required.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.

Usage Guidelines

The **static** command allows you to create a persistent, one-to-one address translation rule (called a static translation slot or “xlate”).

Note The number of address translations allowed is per each FWSM. The FWSM supports 2,048 address translations for the **nat** command, 1,051 address translations for the **global** command, and 2,048 address translations for the **static** command.The FWSM also supports up to 4,096 access control entries (ACEs) in ACLs used for policy NAT.

Note You cannot configure more then 4000 static entries across all contexts.

The embryonic connections per host is set to a small value for slower systems, and a higher value for faster systems. The embryonic connection limit lets you prevent a type of attack where processes are started without being completed. When the embryonic limit is surpassed, the TCP intercept feature intercepts TCP synchronization (SYN) packets from clients to servers on a higher security level. The software establishes a connection with the client on behalf of the destination server, and if successful, establishes the connection with the server on behalf of the client and combines the two half-connections together transparently. The connection attempts from the unreachable hosts never reach the server. The firewall accomplishes TCP intercept functionality using SYN cookies.

This keyword does not apply to outside NAT. The TCP intercept feature applies only to hosts or servers on a higher security level. If you set the embryonic limit for outside NAT, the embryonic limit is ignored. This translation can be between a local IP address and a global IP address (static NAT) or between ports (static PAT). The FWSM dynamically creates a secondary xlate using the global address in the **static** command. This example redirects the FTP service from address 198.168.1.1 to inside host 10.1.1.1 where the address translation slots (xlates) that are necessary for FTP data transfers are automatically created from the global address 192.168.1.1 by the **fixup** application inspection:

```
static (inside, outside) tcp 192.168.1.1 ftp 10.1.1.1 ftp
fixup protocol ftp 21
```

To allow an external host to initiate traffic to an inside host, a static translation rule needs to exist for the inside host. Without the persistent translation rule, the translation cannot occur.

Use the **static** and **access-list** commands when you are accessing the interface of a higher security level from an interface of a lower security level; for example, use these commands when you are accessing the inside interface from a perimeter or the outside interface.

After changing or removing the **static** command, enter the **clear xlate** command.

You can create a single mapping between the global and local hosts, or you can create a range of statics known as net statics.

The **static** command determines the network mask of network statics by the **netmask** keyword or by the number in the first octet of the global IP address. You can use the **netmask** keyword to override the number in the first octet. If the address is all zeros where the net mask is zero, then the address is a net address.

Note Do not create statics with overlapping global IP addresses.

In both the **nat** and **static** statements, the *udp_max_conn* field is applicable even when the TCP *max_conns* limit is not set, by using the keyword **udp**. This allows the two limits to be exclusively configured. This feature is known as policy NAT. The subnet mask used in the access list is also used for the *global_ip*. You can include only the **permit** statements in the access list.

Use the **norandomseq** keyword if another inline firewall is also randomizing sequence numbers and the result is scrambling the data. Without this protection, the inside hosts with weak self-ISN protection become more vulnerable to TCP connection hijacking.

Note The **norandomseq** keyword does not apply to outside NAT. The firewall randomizes only the ISN that is generated by the host/server on the higher security interface. If you set **norandomseq** for outside NAT, the **norandomseq** keyword is ignored.

Idle connections are closed after the time specified by the **timeout connection** command.

Examples

This example shows how to permit a finite number of users to call in through H.323 using Intel Internet Phone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, or Microsoft NetMeeting. The **static** command maps addresses 209.165.201.1 through 209.165.201.30 to local addresses 10.1.1.1 through 10.1.1.30 (209.165.201.2 maps to 10.1.1.2, 209.165.201.10 maps to 10.1.1.10, and so on).

```
fwsm/context_name(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask
255.255.255.224
```

```
fwsm/context_name(config)# access-list acl_out permit tcp any 209.165.201.0
255.255.255.224 eq h323
fwsm/context_name(config)# access-group acl_out in interface outside
```

This example shows the commands that are used to disable Mail Guard:

```
fwsm/context_name(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask
255.255.255.255
fwsm/context_name(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
fwsm/context_name(config)# access-group acl_out in interface outside
fwsm/context_name(config)# no fixup protocol smtp 25
```

In the example, the **static** command allows you to set up a global address to permit outside hosts access to the 10.1.1.1 mail server host on the dmz1 interface. You shoud set the MX record for DNS to point to the 209.165.201.1 address so that mail is sent to this address. The **access-list** command allows the outside users to access the global address through the SMTP port (25). The **no fixup protocol** command disables Mail Guard.

Related Commands

access-list deny-flow-max
global
nat

summary-address

To create the aggregate addresses for OSPF, use the **summary-address** command. To return to the default setting, use the **no** form of this command.

summary-address *addr netmask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr netmask*

Syntax Description

addr	Value of the summary address that is designated for a range of addresses.
netmask	IP address mask or IP subnet mask that is used for a summary route.
not-advertise	(Optional) Sets the address range status to DoNotAdvertise.
tag *tag_value*	(Optional) Specifies the value to match (for controlling redistribution with route maps).

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The type 3 summary LSA is suppressed, and the component networks remain hidden from other networks.

In the **summary-address** command, the **not-advertise** keyword suppresses the routes that match the specified prefix or mask pair.

Examples

This example shows how to create the aggregate addresses for OSPF:

```
fwsm/context_name(config)# summary-address 255.255.255.0 not-advertise
```

Related Commands

router ospf
show ip ospf
show summary-address

sysopt

To change the FWSM system options, use the **sysopt** command. To restore the system options, use the **no** form of this command.

[**no**] **sysopt connection** {**permit-ipsec** | **timewait** | {**tcpmss** [**minimum**] *bytes* } | {**zombie-timeout** [seconds]}}

[**no**] **sysopt nodnsalias inbound | outbound**

[**no**] **sysopt noproxyarp** *interface_name*

[**no**] **sysopt radius ignore-secret**

Syntax Description

connection	Specifies the connection to change.
permit-ipsec	Exempts IPSec traffic from the access check.
timewait	Specifies that the TCP connections undergo the TIMEWAIT state.
tcpmss	Sets the maximum limit of the TCP MSS bytes.
minimum	(Optional) Sets the mimimum limit of the TCP MSS bytes.
bytes	Specifies the byte count for **tcpmss** and **minimum**.
zombie-timeout	Sets the zombie timeout.
seconds	(Optional) Zombie timeout.
nodnsalias inbound	Disables alias inbound DNS A record translation.
nodnsalias outbound	Disables alias outbound DNS A record translation.
noproxyarp *interface_name*	Disables proxy ARP on the specified interface.
radius ignore-secret	Ignores secret in RADIUS accounting responses.

Defaults

bytes is 1380.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **sysopt** command allows you to tune various FWSM security and configuration features. In addition, you can use this command to disable the FWSM IP fragmentation guard.

Examples

This example shows how to display the default sysopt configuration:

```
fwsm(config)# show sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt uauth allow-http-cache
no sysopt connection permit-ipsec
no sysopt connection permit-pptp
no sysopt connection permit-l2tp
no sysopt ipsec pl-compatible
```

This example shows that a PPTP client authenticates using MS-CHAP negotiates MPPE encryption, receives the DNS and WINS server addresses, and connects through Telnet to the host 192.168.0.2 directly through the **nat 0** command:

```
fwsm/context_name(config)# aaa-server my-aaa-server-group (inside) host 192.168.0.10 key
12345678
fwsm/context_name(config)# aaa-server my-aaa-server-group protocol radius
fwsm/context_name(config)# vpdn group 1 accept dialin pptp
fwsm/context_name(config)# vpdn group 1 ppp authentication mschap
fwsm/context_name(config)# vpdn group 1 ppp encryption mppe auto required
fwsm/context_name(config)# vpdn group 1 client configuration address local my-addr-pool
fwsm/context_name(config)# vpdn group 1 client authentication aaa my-aaa-server-group
fwsm/context_name(config)# vpdn group 1 client configuration dns 10.2.2.99
fwsm/context_name(config)# vpdn group 1 client configuration wins 10.2.2.100
fwsm/context_name(config)# vpdn enable outside
fwsm/context_name(config)# access-list nonat permit ip 10.1.1.0 255.255.255.0 host
192.168.0.2
fwsm/context_name(config)# access-list nonat permit ip 10.1.1.0 255.255.255.0 host
10.2.2.99
fwsm/context_name(config)# access-list nonat permit ip 10.1.1.0 255.255.255.0 host
10.2.2.100
fwsm/context_name(config)# nat (inside) 0 access-list nonat
fwsm/context_name(config)# sysopt connection permit-pptp
```

This example shows a minimal IPSec configuration to enable a session to be connected from host 172.21.100.123 to host 172.21.200.67 across an IPSec tunnel that terminates from peer 209.165.201.1 to peer 201.165.200.225.

This example shows how to use the **sysopt connection permit-ipsec** and **access-list** commands on peer 209.165.201.1:

```
fwsm/context_name(config)# static 172.21.100.123 172.21.100.123
fwsm/context_name(config)# access-list 10 permit ip host 172.21.200.67 host 172.21.100.123
fwsm/context_name(config)# crypto ipsec transform-set t1 esp-des esp-md5-hmac
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 10
fwsm/context_name(config)# crypto map mymap 10 set transform-set t1
fwsm/context_name(config)# crypto map mymap 10 set peer 172.21.200.1
fwsm/context_name(config)# crypto map mymap interface outside
```

This example shows how to use the **sysopt connection permit-ipsec** and **access-list** commands on peer 201.165.200.225:

```
fwsm/context_name(config)# static 172.21.200.67 172.21.200.67
fwsm/context_name(config)# access-list 10 permit ip host 172.21.100.123 host 172.21.200.67
fwsm/context_name(config)# crypto ipsec transform-set t1 esp-des esp-md5-hmac
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 10
fwsm/context_name(config)# crypto map mymap 10 set transform-set t1
fwsm/context_name(config)# crypto map mymap 10 set peer 172.21.100.1
fwsm/context_name(config)# crypto map mymap interface outside
```

This command shows how to use the **sysopt connection permit-ipsec** commands on peer 209.165.201.1:

```
fwsm/context_name(config)# static 172.21.100.123 172.21.100.123
fwsm/context_name(config)# access-list 10 permit ip host 172.21.200.67 host 172.21.100.123
fwsm/context_name(config)# crypto ipsec transform-set t1 esp-des esp-md5-hmac
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 10
fwsm/context_name(config)# crypto map mymap 10 set transform-set t1
fwsm/context_name(config)# crypto map mymap 10 set peer 172.21.200.1
fwsm/context_name(config)# crypto map mymap interface outside
fwsm/context_name(config)# sysopt connection permit-ipsec
```

This command shows how to use the **sysopt connection permit-ipsec** commands on peer 201.165.200.225:

```
fwsm/context_name(config)# static 172.21.200.67 172.21.200.67
fwsm/context_name(config)# access-list 10 permit ip host 172.21.100.123 host 172.21.200.67
fwsm/context_name(config)# crypto ipsec transform-set t1 esp-des esp-md5-hmac
fwsm/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsm/context_name(config)# crypto map mymap 10 match address 10
fwsm/context_name(config)# crypto map mymap 10 set transform-set t1
fwsm/context_name(config)# crypto map mymap 10 set peer 172.21.100.1
fwsm/context_name(config)# crypto map mymap interface outside
fwsm/context_name(config)# sysopt connection permit-ipsec
```

Related Commands

alias
ca authenticate
crypto ipsec security-association lifetime
crypto map client
dynamic-map
isakmp

telnet

To add Telnet access to the FWSM console and set the idle timeout, use the **telnet** command. To remove Telnet access from a previously set IP address, use the **no** form of this command.

[**no**] **telnet** *local_ip mask interface_name*

telnet timeout *number*

Syntax Description

local_ip	IP address of a host or network that can access the FWSM Telnet console.
mask	Netmask for the local IP.
interface_name	Network interface name.
timeout *number*	Specifies the number of minutes that a Telnet session can be idle before being closed by the FWSM; valid values are from 1 to 1440 minutes.

Defaults

number is **5** minutes.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **telnet** command allows you to specify which hosts can access the FWSM console with Telnet. You can enable Telnet to the FWSM on all interfaces. However, the FWSM enforces that all Telnet traffic to the outside interface is protected by IPSec. To enable a Telnet session to the outside interface, configure IPSec on the outside interface to include IP traffic that is generated by the FWSM and enable Telnet on the outside interface.

Up to 16 hosts or networks are allowed access to the FWSM console with Telnet, and up to 5 hosts are allowed access to the FWSM simultaneously. Use the **no telnet** or **clear telnet** command to remove Telnet access from a previously set IP address. Use the **telnet timeout** command to set the maximum time that a console Telnet session can be idle before being logged off by the FWSM. The **clear telnet** command does not affect the **telnet timeout** command duration. You cannot use the **no telnet** command with the **telnet timeout** command.

To limit access to a single IP address, use 255 in each octet; for example, 255.255.255.255. You must specify *netmask* as 255.255.255.255 regardless of the class of *local_ip*. Do not use the subnetwork mask of the internal network. The *netmask* is only a bit mask for the IP address in *ip_address*.

If IPSec is operating, you can specify an unsecure interface name, which is typically, the outside interface. At a minimum, you might configure the **crypto map** command to specify an interface name with the **telnet** command.

You must specify an interface namee. The FWSM automatically verifies the IP address against the IP addresses that are specified by the **ip address** commands to ensure that the address that you specify is on an internal interface. If an interface name is specified, the FWSM checks only the host against the interface that you specify.

Use the **passwd** command to set a password for Telnet access to the console. The default is **cisco**. Use the **who** command to view which IP addresses are currently accessing the FWSM console. Use the **kill** command to terminate an active Telnet console session.

If you use the **aaa** command with the **console** keyword, Telnet console access must be authenticated with an authentication server.

Note If you have configured the **aaa** command to require authentication for FWSM Telnet console access and the console login request times out, you can gain access to the FWSM from the serial console by entering the **fwsm** username and the password that was set with the **enable password** command.

Examples

This example shows how to permit hosts 192.168.1.3 and 192.168.1.4 to access the FWSM console through Telnet. In addition, all the hosts on the 192.168.2.0 network are given access.

```
fwsm/context_name(config)# telnet 192.168.1.3 255.255.255.255 inside
fwsm/context_name(config)# telnet 192.168.1.4 255.255.255.255 inside
fwsm/context_name(config)# telnet 192.168.2.0 255.255.255.0 inside
fwsm/context_name(config)# show telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

This example shows how to remove individual entries with the **no telnet** command or all **telnet** commands with the **clear telnet** command:

```
fwsm/context_name(config)# no telnet 192.168.1.3 255.255.255.255 inside
fwsm/context_name(config)# show telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
fwsm/context_name(config)# clear telnet
fwsm/context_name(config)# show telnet
```

This example shows how to change the maximum session idle duration:

```
fwsm/context_name(config)# telnet timeout 10
fwsm/context_name(config)# show telnet timeout
telnet timeout 10 minutes
```

This example shows a Telnet console login session (the password does not display when entered):

```
fwsm# passwd: cisco

Welcome to the FWSM
…
Type help or '?' for a list of available commands.
fwsm>
```

Related Commands

aaa accounting
kill
password/passwd
ssh
who

terminal

To set the terminal line parameter settings, use the **terminal** command.

terminal width *columns*

terminal monitor

terminal [**no**] **monitor**

Syntax Description

width *columns*	Sets the width for displaying information during console sessions; permissible values are 0, which means 511 columns, or a value in the range of 40 to 511.
monitor	Specifies that syslog messages are displayed on this terminal.
no	(Optional) Disables syslog message that displays to this terminal.

Defaults

Width is 80 columns. No monitoring is the default.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode and configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **terminal monitor** command allows you to enable or disable the display of syslog messages in the current session for either Telnet or serial access to the FWSM console. Use the **logging monitor** command to enable or disable various levels of syslog messages to the console; use the **terminal no monitor** command to disable the messages on a per-session basis. Use the **terminal monitor** command to restart the syslog messages for the current session.

The **terminal width** command allows you to set the width for displaying command output. The terminal width is controlled by the **terminal width** *nn* command, where *nn* is the width in characters. If you enter a line break, you cannot use the backspace key to return to the previous line.

Examples

This example shows how to enable logging and then disable logging only in the current session:

```
fwsm/context_name(config)# terminal monitor
fwsm/context_name(config)# terminal no monitor
```

Related Commands

clear terminal
logging
show terminal

tftp-server

To specify the default TFTP server address and directory, use the **tftp-server** command. To disable access to the server, use the **no** form of this command.

[**no**] **tftp-server** *interface_name ip_address directory*

Syntax Description

interface_name	Interface name designated by the **nameif** command.
ip	IP address of the TFTP server.
directory	Directory of the configuration file.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **tftp-server** command allows you to specify the IP address of the server that you use to propagate the FWSM configuration files to the FWSM. Use the **tftp-server** command with the **configure net** command to read from the configuration or with the **write net** command to store the configuration in the file that you specify. The FWSM supports only one TFTP server.

The *path* name that you specify in the **tftp-server** is appended to the end of the IP address that you specify in the **configure net** and **write net** commands. Because the *path* name is appended to the IP address that you specify with the **tftp-server** command, you will not need to specify the file and pathname with the **configure net** and **write net** commands. If you specify the full *path* and filename in the **tftp-server** command, the IP address in the **configure net** and **write net** commands can be represented with a colon (**:**).

This is the interface by which the TFTP server IP is accessible.

The *interface_name* argument specifies the interface name designated by the **nameif** command. If you specify the outside interface, a warning message informs you that the outside interface is unsecure.

Caution Specifying an unsecure interface may put your data at a security risk.

The format for *path* differs by the type of operating system of the server that you are using to contain the configuration files for the FWSM. The contents of a path are passed directly to the server without interpretation or checking. The configuration file must exist on the TFTP server. Many TFTP servers require the configuration file to be world-writable to write to it and world-readable to read from it.

Note If the TFTP server to which the FWSM is trying to connect is not running TFTP, the FWSM suspends operation and does not time out. Press the **ESC** key on the FWSM console to abort the TFTP session and return to the command-line prompt.

Examples

This example shows how to specify a TFTP server and then read the configuration from /FWSM/config/test_config directory:

```
fwsm/context_name(config)# tftp-server inside 10.1.1.42 /fwsm/config/test_config
fwsm/context_name(config)# configure net :
```

Related Commands

clear tftp-server
show tftp-server

timeout

To set the maximum idle time duration, use the **timeout** command.

timeout [**xlate** | **conn** | **udp** | **icmp** | **rpc** | **h323** | **h225** | **mgcp** | **sip** | **sip_media** | **uauth** *hh*:*mm*:*ss*]

Syntax Description

xlate	(Optional) Specifies the idle time until a translation slot is freed; the minimum value is 1 minute.
conn	(Optional) Specifies the idle time after which a connection closes; the minimum duration is 5 minutes.
udp	(Optional) Specifies the idle time until a UDP slot is freed; the minimum duration is 1 minute.
icmp	(Optional) Specifies the idle time after which general ICMP states are closed.
rpc	(Optional) Specifies the idle time until an RPC slot is freed; the minimum duration is 1 minute.
h323	(Optional) Specifies the idle time after which an H323 control connection is closed.
h255	(Optional) Specifies the idle time after which H.225 signaling closes.
mgcp	(Optional) Sets the duration for the Media Gateway Control Protocol (MGCP) inactivity timer.
sip	(Optional) Modifies the SIP timer.
sip_media	(Optional) Modifies the media timer, which is used for SIP RTP/RTCP with SIP UDP media packets, instead of the UDP inactivity timeout.
uauth	(Optional) Sets the duration before the authentication and authorization cache times out and the user has to reauthenticate the next connection.
hh:*mm*:*ss*	Timeout.

Defaults

The defaults are as follows:

- **xlate** *hh*:*mm*:*ss* is 3 hours (**03:00:00**).
- **conn** *hh*:*mm*:*ss* is 1 hour (**01:00:00**).
- **half-closed** *hh*:*mm*:*ss* is 10 minutes (**00:10:00**).
- **udp** *hh*:*mm*:*ss* is 2 minutes (**00:02:00**).
- **rpc** *hh*:*mm*:*ss* is 10 minutes (**00:10:00**).
- **h255** *hh*:*mm*:*ss* is 1 hour (**01:00:00**).
- **h323** *hh*:*mm*:*ss* is 5 minutes (**00:05:00**).
- **mgcp** *hh:mm:ss* is 5 minutes (**00:05:00**).

- **sip** *hh:mm:* is 30 minutes (**00:30:00**).
- **sip_media** *hh:mm:ss* is 2 minutes (**00:02:00**).
- **uauth** timer is **absolute**.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **timeout** command allows you to set the idle time for connection, translation UDP, and RPC slots. If the slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

Note The maximum configurable value for timeout connections is 18 hours.

This command is used with the **show** and **clear uauth** commands.

Note Do not use the **timeout uauth 0:0:0** command if passive FTP is used for the connection or if the **virtual** command is used for web authentication.

The connection timer takes precedence over the translation timer; the translation timer works only after all connections have timed out.

When setting the **conn** *hh*:*mm*:*ss*, use **0:0:0** to never time out a connection.

When setting the **half-closed** *hh*:*mm*:*ss*, use **0:0:0** to never time out a half-closed connection.

When setting the **h255** *hh*:*mm*:*ss*, **h225 00:00:00** means to never tear down H.225 signaling. A timeout value of **h225 00:00:01** disables the timer and closes the TCP connection immediately after all calls are cleared.

The **uauth** *hh*:*mm*:*ss* duration must be shorter than the **xlate** keyword. Set to **0** to disable caching. Do not set to zero if passive FTP is used on the connections.

To disable the **absolute** keyword, set the uauth timer to 0 (zero).

Caution Be careful when using the remote procedure call (RPC) and Network File System (NFS) protocols because they are unsecure protocols.

Examples

This example shows how to configure the maximum idle time durations:

```
fwsm/context_name(config)# timeout uauth 0:5:00 absolute uauth 0:4:00 inactivity
fwsm/context_name(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

Related Commands

arp
clear timeout
show timeout
show xlate
show uauth

timers

To configure the OSPF process delay timers, use the **timers** command. To return to the default settings, use the **no** form of this command.

timers {**spf** *spf_delay spf_holdtime* | **lsa-group-pacing** *seconds*}

no timers {**spf** | **lsa-group-pacing**}

Syntax Description

spf *spf_delay*	Specifies the delay time between when OSPF receives a topology change and when it starts a shortest path first (SPF) calculation in seconds, from 0 to 65535.
spf_holdtime	The hold time between two consecutive SPF calculations in seconds; valid values are from 1 to 65534.
lsa-group-pacing *seconds*	Specifies the delay time between when OSPF receives a topology change and when it starts a calculation, and the hold time between two consecutive SPF calculations; valid values are from 10 to 1800 seconds.

Defaults

The defaults are as follows:

- *spf_delay* is **5** second.
- *spf_holdtime* is **10** seconds.
- *seconds* is **240** seconds.

Command Modes

Security Context Mode: single context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: Routed

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

To configure the delay time between when the OSPF protocol receives a topology change and when it starts a calculation, and the hold time between two consecutive SPF calculations, use the **timers spf** *spf_delay spf_holdtime* subcommand. To return to the default timer values, use the **no timers spf** subcommand.

To change the interval at which the OSPF link-state advertisements (LSAs) are collected into a group and refreshed, checksummed, or aged, use the **timers lsa-group-pacing** *seconds* subcommand. To return to the default timer values, use the **no timers lsa-group-pacing** subcommand.

Examples

This example shows how to configure OSPF process delay timers:

```
fwsm/context_name(config)# timers lsa-group-pacing 40
```

Related Commands

router ospf
show ip ospf
show timers

upgrade-mp

To upgrade the maintenance partition, use the **upgrade-mp** command.

upgrade-mp tftp://*location/pathname*

upgrade-mp http[**s**]**://**[*user*:*password*@]*location* [:*port*]/*pathname*

upgrade-mp tftp[:[[**//***location*][/*pathname*]]]

Syntax Description

location	(Optional) Location of the upgrade software image.
pathname	(Optional) Pathname to the upgrade software image.
user	(Optional) Username.
password	(Optional) User's password.
port	HTTP port.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system command line

Command Mode: privileged mode and configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Examples

This example show how to configure a route map for use in OSPF routing:

```
fwsm(config)# upgrade-mp tftp://10.192.1.1/c6svc-mp.2-1-1.bin.gz
```

uptime

To display the FWSM version and the time that the module has been running, use the **uptime** command.

uptime

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.
2.3(1)	This command is not supported in this release. The **show uptime** command is supported.

Examples

This example shows how to display FWSM version and runtime information:

```
FWSM# show uptime
FWSM Firewall Version 2.3(1)11
FWSM Device Manager Version 4.0(1)
Compiled on <?xml:namespace prefix = st1 ns = "urn:schemas-microsoft-com:office:smarttags"
/>Fri 04-Feb-05 00:12 by dalecki
FWSM up 6 hours 21 mins
Hardware:   WS-SVC-FWM-1, 1024 MB RAM, CPU Pentium III 1000 MHz
Flash  V1.01   SMART ATA FLASH DISK @ 0xc321, 20MB
0: gb-ethernet0: irq 5
1: gb-ethernet1: irq 7
2: ethernet0: irq 11
Licensed Features:
Failover:           Enabled
VPN-DES:            Enabled
VPN-3DES:           Enabled
Maximum Interfaces: 256
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Throughput:         Unlimited
ISAKMP peers:       Unlimited
```

Related Commands

show uptime

url-block

To enable long URL support and HTTP response buffering for URL filtering services, use the **url-block** command. To disable long URL support and HTTP response buffering for URL filtering services, use the **no** form of this command.

[**no**] **url-block** {**block** *block_buffer_limit*} | {**url-mempool** *memory_pool_size*} | {**url-size** *long_url_size*}

Syntax Description

block *block_buffer_limit*	Specifies the maximum number of blocks that are allowed in the HTTP response buffer, valid values are from 1 to 128.
url-mempool *memory_pool_size*	Specifies the size of the URL buffer memory pool in Kilobytes (KB); valid values are from 2 to 10240 KB.
url-size *long_url_size*	Specifies the maximum allowed URL size in KB; valid values are from 2 to 4 KB.

Defaults

block_buffer_limit is **1** KB.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **url-block url-size** *long_url_size* command is supported on Websense servers only.

The **url-block** command requires that a valid Websense URL filtering configuration is running on the FWSM. After a valid Websense URL filter is in place, you can use this command to pass the URLs that are longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense server. The **url-block** command stores the URLs that are longer than 1159 bytes in a buffer and then passes the URL to the Websense server (through a TCP packet stream) so that the Websense server can grant or deny access to that URL.

Examples

This example shows how to enable long URL support and HTTP response buffering for URL filtering services:

```
FWSM(config)# url-block block 128
FWSM(config)# url-block url-mempool 1500
FWSM(config)# url-block url-size 4
```

Related Commands

clear url-block
show url-block

url-cache

To cache web server responses that are pending a permit or deny response from an N2H2 server or Websense server, use the **url-cache** command. To disable caching, use the **no** form of this command.

[**no**] **url-cache** {**dst** | **src_dst**} **size** *kbytes*

Syntax Description

dst	Specifies cache entries that are based on the URL destination address.
src_dst	Specifies cache entries that are based on the both the source address initiating the URL request as well as the URL destination address.
size *kbytes*	Specifies a value for the cache size within the range 1 to 128 KB.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **url-cache** command provides a configuration option to buffer the response from a web server if its response is faster than that from the N2H2 or Websense filtering service server. This command prevents the web server's response from being loaded twice.

When you access a site, the filtering server can allow the FWSM to cache the server address for a certain amount of time, as long as every site hosted at the address is in a category that is permitted at all times. When you access the server again, or if another user accesses the server, the FWSM does not need to consult the filtering server.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display the cache statistics.

Caching stores URL access privileges in memory on the FWSM. When a host requests a connection, the FWSM first looks in the URL cache for matching access privileges instead of forwarding the request to the N2H2 or Websense server. You can disable caching with the **no url-cache** command.

Using the URL cache does not update the Websense accounting logs for Websense protocol version 1. If you are using Websense protocol version 1, you should allow Websense to accumulate logs so that you can view the Websense accounting information. After you get a usage profile that meets your security needs, you can enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol version 4 and for N2H2 URL filtering while using the **url-cache** command.

Note If you change the settings on the N2H2 or Websense server, disable the cache with the **no url-cache** command and then reenable the cache with the **url-cache** command.

Select **dst** mode if all users share the same URL filtering policy on the N2H2 or Websense server.

Select **src_dst** mode if the users do not share the same URL filtering policy on the N2H2 or Websense server.

Examples

This example shows how to cache all outbound HTTP connections that are based on the source and destination addresses:

```
fwsm/context_name(config)# url-cache src_dst 128
```

Related Commands

clear url-cache
show url-cache stat

url-server

To designate a server running either N2H2 server or Websense servers for use with the **filter** command, use the **url-server** command. To remove the server, use the **no** form of this command.

N2H2 Commands

url-server {*interface_name*} **vendor n2h2 host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** | **UDP**}]

no url-server {*interface_name*} **vendor n2h2 host** *local_ip* [**port** *number*] [**timeout** *seconds*] [**protocol** {**TCP** | **UDP**}]

Websense Commands

url-server {*interface_name*} **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP**} *version*]

no url-server {*interface_name*} **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP**} *version*]

Syntax Description

N2H2

interface_name	Network interface where the authentication server resides. If not specified, the default is inside.
vendor n2h2	Indicates that the URL filtering service vendor is N2H2.
host *local_ip*	IP address of the local server that runs the URL filtering application.
port *number*	(Optional) Specifies the N2H2 filtering application server port number.
timeout *seconds*	(Optional) Specifies the maximum idle time permitted before the FWSM switches to the next server that you specified.
protocol TCP	(Optional) Specifies the TCP protocol.
protocol UDP	(Optional) Specifies the UDP protocol.

Websense

interface_name	Network interface where the authentication server resides.
vendor websense	Indicates that the URL filtering service vendor is Websense.
host *local_ip*	IP address of the local server that runs the URL filtering application.
timeout *seconds*	(Optional) Specifies the maximum idle time that is permitted before the FWSM switches to the next server specified.
protocol TCP	(Optional) Specifies the TCP protocol.
protocol UDP	(Optional) Specifies the UDP protocol.
version	(Optional) Protocol version 1 or 4.

Defaults

The default settings for the N2H2 filtering application are as follows:

- If not specified, the *interface_name* is inside.
- **port** *number* is **4005**.
- **timeout** *seconds* is **5** seconds.
- **protocol** is TCP.

The default settings for Websense are as follows:

- If not specified, the *interface_name* is inside.
- **timeout** *seconds* is **5** seconds.
- **protocol** is TCP.
- *version* is TCP version 1.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **url-server** command allows you to designate the server running the N2H2 server or Websense server URL. The FWSM supports four URL servers per context in multiple mode; 16 URL servers can be assigned in single mode. However, you can use only one application at a time, either the N2H2 server or the Websense server. Changing the configuration on the FWSM does not update the configuration on the application server. Changing the configuration must be done separately and according to the individual vendor's instructions.

Note For information about filtering by the N2H2 server, refer to this URL:
http://www.n2h2.com.
For information on Websense filtering services, refer to this URL:
http://www.websense.com/

You must configure the **url-server** command before using the **filter** command for HTTPS and FTP. If you remove all URL servers from the server list, then all **filter** commands that are related to URL filtering are also removed.

You cannot run both URL filtering services simultaneously.

For Websense, you can configure TCP using version 1 or version 4. You can configure UDP using version 4 only.

Examples

This example shows how to filter all outbound HTTP connections except those from the 10.0.2.54 host when using N2H2:

```
fwsm/context_name(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
fwsm/context_name(config)# filter url http 0 0 0 0
fwsm/context_name(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

This example shows how to filter all outbound HTTP connections except those from the 10.0.2.54 host when using Websense:

```
fwsm/context_name(config)# url-server (perimeter) vendor websense host 10.0.1.1
fwsm/context_name(config)# filter url http 0 0 0 0
fwsm/context_name(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

aaa authorization
clear url-server
filter ftp
show url-server

username

To set the username for the specified privilege level, use the **username** command. To remove the username and privilege level, use the **no** form of this command.

username *username* {[{**nopassword** | **password** *password*} [**encrypted**]] [**privilege** *level*]}

no username *username*

Syntax Description

username	Name of a specific user in the local FWSM authentication database.
nopassword	(Optional) Specifies that password access is not required.
password *password*	(Optional) Specifies that password access is required and specifies a password.
encrypted	(Optional) Specifies encryption.
privilege *level*	(Optional) Specifies the privilege level for the user.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The local FWSM user authentication database consists of the users entered with the **username** command. The FWSM **login** command uses this database for authentication.

Examples

This example shows how to set the username for the specified privilege level:

```
fwsm/context_name(config)# username larry nopassword privilege 4
```

Related Commands

clear username
login
privilege
show username

virtual

To access the FWSM virtual server, use the **virtual** command.

virtual http *ip_address* [**warn**]

virtual telnet *ip_address*

Syntax Description

http	Allows web browsers to work correctly with the FWSM **aaa** command. See the "Usage Guidelines" section for additional information.
ip_address	IP address. See the "Usage Guidelines" section for additional information.
warn	(Optional) Notifies the **virtual http** command users that the command was redirected.
telnet	Logs you in and logs you out of the FWSM. See the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **virtual http** command allows web browsers to work correctly with the FWSM **aaa** command. The **aaa** command assumes that the AAA server database is shared with a web server. The FWSM automatically provides the AAA server and web server with the same information. The **virtual http** command works with the **aaa** command to authenticate the user, separate the AAA server information from the web client's URL request, and direct the web client to the web server. Use the **show virtual http** command to list the commands in the configuration. Use the **no virtual http** command to disable its use.

The **virtual http** command allows you to redirect the web browser's initial connection to the *ip_address,* which resides in the FWSM, authenticating the user, and then redirecting the browser to the URL that the user originally requested. The **virtual http** command accesses the virtual server for use with HTTP. This command is useful for FWSM interoperability with Microsoft IIS and for other authentication servers.

When using HTTP authentication to a site running Microsoft IIS that has "Basic text authentication" or "NT Challenge" enabled, users may be denied access from the Microsoft IIS server because the browser appends the string: "Authorization: Basic=Uuhjksdkfhk==" to the HTTP GET commands. This string contains the FWSM authentication credentials.

For outbound use, the *ip_address* must be entered as an address routed to the FWSM.

For inbound use, the *ip_address* must be entered as an unused global address.

Caution Do not set the **timeout uauth** duration to 0 seconds when using the **virtual** command because this action will prevent HTTP connections to the real web server.

The **virtual telnet** command allows the Virtual Telnet server to provide a way to preauthenticate users who require connections through the FWSM using services or protocols that do not support authentication.

You can use the **virtual telnet** command both to log in and log out of the FWSM. When an unauthenticated user connects through Telnet to the virtual IP address, that user is challenged for a username and password, and then authenticated with the TACACS+ or RADIUS server. Once authenticated, the user sees the message "Authentication Successful" and the authentication credentials are cached in the FWSM for the duration of the uauth timeout.

The Virtual Telnet server provides a way to preauthenticate users who require connections through the FWSM using services or protocols that do not support authentication. Users first connect to the Virtual Telnet server IP address, where the user is prompted for a username and password.

The **warn** keyword is applicable only for text-based browsers where the redirect cannot happen automatically.

Examples

This example shows how to make an inbound connection:

```
fwsm/context_name(config)# static (inside, outside) 209.165.201.1 209.165.201.1 netmask
255.255.255.255
fwsm/context_name(config)# access-list acl_out permit tcp any host 209.165.201.1 eq 80
fwsm/context_name(config)# access-group acl_out in interface outside
fwsm/context_name(config)# aaa authentication include any inbound 209.165.201.1
255.255.255.255 0 0 tacacs+
fwsm/context_name(config)# virtual http 209.165.201.1
```

This example displays the **show virtual** command output:

```
fwsm(config)# show virtual http
virtual http 209.165.201.1
```

After adding the **virtual telnet** command to the configuration and writing the configuration to the Flash partition, the users wanting to start Point-to-Point Tunneling (PPTP) sessions through the FWSM use Telnet to access the *ip_address*.

This example shows how to make a connection to the FWSM:

```
fwsm/context_name(config)# virtual telnet 209.165.201.25
fwsm/context_name(config)# aaa authentication include any outside 209.165.201.1
255.255.255.0 0 tacacs+
fwsm/context_name(config)# static (inside, outside) 209.165.201.25 209.165.201.25 netmask
255.255.255.255
fwsm/context_name(config)# access-list acl_out permit tcp any host 209.165.201.25 eq
telnet
fwsm/context_name(config)# access-group acl_out in interface outside
fwsm/context_name(config)# write memory
```

This example shows how to make a connection to an inside host:

```
fwsm(config)# /unix/host%telnet 209.165.201.30
Trying 209.165.201.25...
Connected to 209.165.201.25.
```

```
Escape character is '^]'.
fwsm(config)# username: username
fwsm(config)# TACACS+ Password: password
Authentication Successful
Connection closed by foreign host.
/unix/host%
```

The *username* and *password* are for the user on the TACACS+ server.

Related Commands

clear virtual

vpngroup

To configure the Cisco VPN client version 3.x (Cisco unified VPN client framework), use the **vpngroup** command.

vpngroup *group_name* {**address-pool** *pool_name*} | {**default-domain** *domain_name*} | {**dns-server** *dns_ip_prim* [*dns_ip_sec*]} | {**idle-time** *idle_seconds*} | {**max-time** *max_seconds*} | {**password** *preshared_key*} | {**split-tunnel** *access_list*} | {**wins-server** *wins_ip_prim* [*wins_ip_sec*]

Syntax Description

group_name	VPN policy group name; the name is an ASCII string with a maximum of 63 characters.
address-pool *pool_name*	Specifies the IP address pool name; the name can be up to 63 characters.
default-domain *domain_name*	Default domain name; the name can be up to 127 characters.
dns-server *dns_ip_prim*	Specifies the IP address of the primary DNS server.
dns_ip_sec	(Optional) IP address of the secondary DNS server.
idle-time *idle_seconds*	Specifies the idle timeout in seconds; valid values are from 60 to 86400 seconds.
max-time *max_seconds*	Specifies the maximum connection time in seconds that the VPN group is allowed; valid values are from 60 to 31536000 seconds.
password *preshared_key*	VPN group preshared key; the maximum is 127 characters.
split-tunnel *access_list*	Specifies the name of the access list for the split-tunnel configuration.
wins-server *wins_ip_prim*	Specifies the IP address of the primary Windows Internet Name Service (WINS) server.
wins_ip_sec	(Optional) IP address of the secondary WINS server.

Defaults

The defaults are as follows:

- *max_seconds* is set to unlimited.
- *idle_seconds* is **1800** seconds (30 minutes).

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: configuration mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Make sure that you configure the Internet Key Exchange (IKE) mode configuration before you configure support for the Cisco VPN Client. Specify that the FWSM initiates the IKE mode configuration.

For additional information about configuring interoperability with the Cisco VPN Client using the **vpngroup** commands, refer to the *Cisco VPN Configuration Guide*. The Cisco VPN Client supports Windows 2000.

The **vpngroup** command set allows you to configure Cisco VPN Client policy attributes to be associated with a VPN group name and are downloaded to the Cisco VPN Client(s) that are part of the given group. The same VPN group name specified here is configured in the Cisco VPN Client to ensure the matching of VPN client.

Configure a VPN group name of "default" to create a VPN group policy that matches any group name. The FWSM selects the VPN group name "default," if there is no other policy match. The VPN *group_name* is an ASCII string to denote a VPN group. You can make up the name. The maximum name has 63 characters.

The **vpngroup address-pool** command allows you to define a pool of local addresses to be assigned to a VPN group.

Note Both the **vpngroup address-pool** command and the **ip local pool** command enable you to specify a pool of local addresses for assigning dynamic IP addresses to VPN clients. For the Cisco VPN Client, the specified pool of addresses is associated with a given group, which consists of Cisco VPN Client users. We recommend that you use the **vpngroup address-pool** command only if you configure more than one pool of addresses to be used by more than one VPN user group. The **vpngroup address-pool** command allows the FWSM to configure different pools of local addresses for different user groups.

Use the **vpngroup** *group_name* **user-idle-timeout** *user_idle_seconds* command to set the IUA idle timeout.

Use the **vpngroup dns-server** command to enable the FWSM to download an IP address of a DNS server to a Cisco VPN Client as part of an IKE negotiation.

The **vpngroup wins-server** command allows the FWSM to download an IP address of a WINS server to a Cisco VPN Client as part of an IKE negotiation.

To enable the FWSM to download a default domain name to a Cisco VPN Client as part of IKE negotiation, use the **vpngroup default-domain** command.

Use the **vpngroup split-tunnel** command to enable split tunneling on the FWSM. Split tunneling allows a remote VPN client simultaneous encrypted access to the corporate network and clear access to the Internet. When you use the **vpngroup split-tunnel** command, specify the access list name to which you are associating split tunneling of traffic. With split tunneling enabled, the FWSM downloads its local network IP address and netmask specified within the associated access list to the VPN client or as part of the policy push to the client. The VPN client sends the traffic that is destined to the specified local FWSM network through an IPSec tunnel and all other traffic in the clear. The FWSM receives the IPSec-protected packet on its outside interface, decrypts it, and then sends it to its specified local network.

The networks defined in the **access-list deny** commands are not pushed to VPN clients.

The **vpngroup idle-time** command allows you to set the inactivity timeout for a Cisco VPN Client. When the inactivity timeout for all IPSec SAs have expired for a given VPN client, the tunnel is terminated.

The **vpngroup max-time** command allows you to set the maximum connection time for a Cisco VPN Client. When the maximum connection time is reached for a given VPN client, the tunnel is terminated. The connection between the Cisco VPN Client and the FWSM has to be reestablished. The default maximum connection time is set to an unlimited amount of time.

Note The inactivity timeout that is specified with the **vpngroup idle-time** command and the maximum connection time that is specified with the **vpngroup max-time** command for a given Cisco VPN Client take precedence over the commands that are used to set global lifetime timeouts. These commands are the **isakmp policy lifetime** and **crypto map set security-association lifetime seconds** commands.

Configure the VPN group's preshared key employing the **vpngroup password** command to be used during IKE authentication. This preshared key is equivalent to the password that you enter within the **Group Password** box of the Cisco VPN Client while configuring your group access information for a connection entry.

The FWSM-configured password displays in asterisks within the file configuration.

Note Both the **vpngroup password** command and the **isakmp key address** command allow you to specify a preshared key for IKE authentication. We recommend that you use the **vpngroup password** command only if you plan to configure more than one VPN user group. The **vpngroup password** command allows the FWSM to configure different VPN user groups.

Examples

This example shows that the VPN client(s) within the VPN group named as "myVpnGroup" is dynamically assigned with one of the IP addresses from the pool of addresses ranging from 10.140.40.0 to 10.140.40.7. The policy attributes for the group "myVpnGroup" are downloaded to the given VPN client during the policy push to the client. Split tunnelling is enabled. All traffic that is destined for the 10.130.38.0 255.255.255.0 FWSM network from the VPN client is protected by IPSec.

```
fwsm/context_name(config)# access-list 90 permit ip 10.130.38.0 255.255.255.0 10.140.40.0
255.255.255.248

fwsm/context_name(config)# ip local pool vpnpool 10.140.40.1-10.140.40.7

fwsm/context_name(config)# crypto ipsec transform-set esp-sha esp-null esp-sha-hmac
fwsm/context_name(config)# crypto dynamic-map dynmap 50 set transform-set esp-sha
fwsm/context_name(config)# crypto map mapName 10 ipsec-isakmp dynamic dynmap
fwsm/context_name(config)# crypto map mapName client configuration address initiate
fwsm/context_name(config)# crypto map mapName interface outside

fwsm/context_name(config)# isakmp enable outside
fwsm/context_name(config)# isakmp identity hostname
fwsm/context_name(config)# isakmp policy 7 authentication pre-share
fwsm/context_name(config)# isakmp policy 7 encryption 3des
fwsm/context_name(config)# isakmp policy 7 hash md5
fwsm/context_name(config)# isakmp policy 7 group 1

fwsm/context_name(config)# vpngroup myVpnGroup address-pool vpnpool
fwsm/context_name(config)# vpngroup myVpnGroup dns-server 10.131.31.11
fwsm/context_name(config)# vpngroup myVpnGroup wins-server 10.131.31.11
fwsm/context_name(config)# vpngroup myVpnGroup default-domain example.com
fwsm/context_name(config)# vpngroup myVpnGroup split-tunnel 90
fwsm/context_name(config)# vpngroup myVpnGroup idle-time 1800
fwsm/context_name(config)# vpngroup myVpnGroup max-time 86400
fwsm/context_name(config)# vpngroup myVpnGroup password ********
```

Related Commands

clear vpngroup
show vpngroup

who

To display active Telnet administration sessions on the FWSM, use the **who** command.

who [*local_ip*]

show who [*local_ip*]

Syntax Description

local_ip	(Optional) Internal IP address to limit the listing to one IP address or to a network IP address.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **who** command allows you to display the FWSM TTY_ID and IP address of each Telnet client that is currently logged into the FWSM. This command is the same as the **show who** command.

Examples

This example shows how to display active Telnet administration sessions on the FWSM:

```
fwsm# who

0: From 192.168.1.3
1: From 192.168.2.2
```

Related Commands

kill
show who
telnet

write

To store, view, or erase the current configuration, use the **write** command.

write net [[*tftp_ip*]:[*filename*]]

write {**erase** | **memory** | **terminal** | **standby**}

Syntax Description

tftp_ip	(Optional) IP address of the TFTP server.
filename	(Optional) Filename to qualify the location of the configuration file on the TFTP server named in *server_ip*.
erase	Clears the Flash partition configuration.
memory	Stores the current configuration in the Flash partition and the activation key value and time stamp for when the configuration was last modified.
terminal	Displays the current configuration on the terminal.
standby	Stores the configuration to the failover standby module from RAM to RAM.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
1.1(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

Note The **write standby** command can be used only if the active and standby FWSMs are configured differently.

The **standby** keyword forces the configuration synchronization from the active to the standby module.

The **write net** command allows you to store the current configuration into a file on a TFTP server elsewhere in the network. The **write net** command allows you to use the TFTP server IP address that is specified in the **tftp-server** command. If you specify both the IP address and pathname in the **tftp-server** command, you can specify the **write net**:*filename* command as a colon (:) as follows:

```
fwsm(config)# write net :
```

If you set a filename with the **tftp-server** command, do not specify it in the **write** command; instead, use a colon (:) without a filename. Many TFTP servers require the configuration file to be world-writable to write to it.

Use the **configure net** command to get the configuration from the file.

The **write erase** command clears the Flash partition configuration.

The **write memory** command saves the current running configuration to the Flash partition. Use the **configure memory** command to merge the current configuration with the image that you saved in the Flash partition.

The FWSM allows processing to continue during the **write memory** command.

If another FWSM console user tries to change the configuration while you are executing the **write memory** command, the user receives this message:

```
Another session is busy writing configuration to memory
Please wait a moment for it to finish
```

After the **write memory** command completes, the FWSM allows the other command to complete.

Note Use the **write memory** command only if a configuration has been created with IP addresses for both network interfaces.

The **write terminal** command displays the current configuration in the FWSM's RAM memory. You can also display the configuration that is stored in the Flash partition by using the **show configure** command.

Defaults

The default on the FWSM is to store all configurations in compressed format.

Examples

This example shows how to specify the TFTP server and create a file named new_config in which to store the configuration:

```
fwsm(config)# tftp-server 10.1.1.2 /fwsmfirewall/config/new_config
write net :
```

This example shows how to erase the contents of the Flash partition and reload the FWSM:

```
fwsm(config)# write erase
Erase fwsm configuration in flash partition? [confirm] y
fwsm(config)# reload
Proceed with reload? [confirm] y
```

This example shows how to save the current configuration to the Flash partition:

```
fwsm(config)# write memory
Building configuration…
[OK]
```

This example shows how to display the configuration:

```
fwsm(config)# write terminal
Building configuration…
: Saved
```

Related Commands

configure

write standby

To force the configuration synchronization from the active to the standby module, use the **write standby** command.

write standby

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system and context command line

Command Mode: privileged mode

Firewall Mode: routed firewall mode and transparent firewall mode

Command History

Release	Modification
2.2(1)	Support for this command was introduced on the FWSM.

Usage Guidelines

The **write standby** command allows you to write the configuration that is stored in RAM on the active failover module to the RAM on the standby module. When the primary module boots, it automatically writes the configuration to the secondary module. Enter the **write standby** command if the primary and secondary module configurations have different information.

Note The **write standby** command can be used only if the active and standby FWSMs are configured differently.

You can use this command in these modes:

- Single Mode—Forces complete configuration synchronization to the standby module.
- Multi-mode, user context—Forces the context configuration to synchronize to the standby module.
- Multi-mode, system context—Forces the complete configuration (system and all user context configuration information) to synchronize to the standby module.

You can also display the configuration that is stored in the Flash partition by using the **show configure** command.

Examples

This example shows how to force the configuration synchronization from the active to the standby module:

```
fwsm(config)# write standby
Building configuration…
[OK]
```

Related Commands

clear failover
configure
failover
failover interface ip
failover interface-policy
failover lan interface
failover lan unit
failover link
failover polltime
failover replication http
failover reset
monitor-interface
show failover
write standby

Acronyms and Abbreviations

This appendix lists the acronyms and abbreviations that are used in this document. Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Command Reference* for information on the commands described in this section.

Table A-1 Acronyms and Abbreviations

Acronym	Description
AAA	authentication, authorization, and accounting.
ABR	Area Border Router.
ACE	access control entry.
ACL	access control list.
AH	Authentication Header.
ARP	Address Resolution Protocol—A low-level TCP/IP protocol that maps a node's hardware address (MAC address) to its IP address. Defined in RFC 826. An example hardware address is 00:00:a6:00:01:ba. (The first three groups specify the manufacturer, and the rest identify the host's motherboard.)
ASBR	Autonomous System Boundary Router.
BGP	Border Gateway Protocol—While the FWSM does not support use of this protocol, you can set the routers on either side of the FWSM to use RIP between them and then run BGP on the rest of the network before the routers.
BOOTP	Bootstrap Protocol—Allows diskless workstations to boot over the network and is described in RFC 951 and RFC 1542.
CA	certification authority.
CHAP	Challenge Handshake Authentication Protocol. Security feature supported on lines using PPP encapsulation that prevents unauthorized access.
chargen	Character Generation—Via TCP, a service that sends a continual stream of characters until stopped by the client. Via UDP, the server sends a random number of characters each time that the client sends a datagram. Defined in RFC 864.
conn	Connection slot.
CPP	Combinet Proprietary Protocol.
CPU	central processing unit.
CRL	certificate revocation list.
CS-ACS	Cisco Secure ACS.

Table A-1 Acronyms and Abbreviations (continued)

Acronym	Description
CTI	Computer Telephony Integration.
CTIQBE	Computer Telephony Interface Quick Buffer Encoding.
dACL	Downloadable ACL.
DES	Data Encryption Standard.
DH	Diffie-Hellman.
DHCP	Dynamic Host Configuration Protocol.
DNS	Domain Name System—Operates over UDP unless zone file access over TCP is required.
DoS	Denial of service.
ECMP	Equal Cost Multi-Path.
EEPROM	Electrically Erasable Programmable Read-Only Memory.
EGP	Exterior Gateway Protocol—While the FWSM does not support use of this protocol, you can set the routers on either side of the FWSM to use RIP between them and then run EGP on the rest of the network before the routers.
EIGRP	Enhanced Interior Gateway Routing Protocol—While the FWSM does not support use of this protocol, you can set the routers on either side of the FWSM to use RIP between them and then run EIGRP on the rest of the network before the routers.
ESP	Encapsulating Security Payload. Refer to RFC 1827 for more information.
FAT	File Allocation Table.
FDDI	Fiber Distributed Data Interface—Fiber optic interface.
FDM	Firewall Device Manager.
FTP	File Transfer Protocol.
FWSM	Firewall Services Module.
gaddr	Global address—An address set with the **global** and **static** commands.
GRE	Generic routing encapsulation protocol—Commonly used with Microsoft's implementation of PPTP.
H.323	A collection of protocols that allow the transmission of voice data over TCP/IP networks.
HSRP	Hot-Standby Routing Protocol.
HTTP	Hypertext Transfer Protocol—The service that handles access to the World Wide Web.
https	HTTP over SSL.
IANA	Internet Assigned Number Authority—Assigns all port and protocol numbers for use on the Internet. You can view port numbers at the following site: http://www.iana.org/assignments/port-numbers You can view protocol numbers at the following site: http://www.iana.org/assignments/protocol-numbers

Table A-1 Acronyms and Abbreviations (continued)

Acronym	Description
ICMP	Internet Control Message Protocol—This protocol is commonly used with the **ping** command. You can view ICMP traces through the FWSM with the **debug trace on** command. Refer to RFC 792 for more information.
IFP	Internet Filtering Protocol.
IGMP	Internet Group Management Protocol.
IGRP	Interior Gateway Routing Protocol.
IKE	Internet Key Exchange.
IKMP	Internet Key Management Protocol.
IP	Internet Protocol.
IPCP	IP Control Protocol. Protocol that establishes and configures IP over PPP.
IPinIP	IP-in-IP encapsulation protocol.
IPSec	IP Security Protocol efforts in the IETF (Internet Engineering Task Force).
IRC	Internet Relay Chat protocol—The protocol that lets users access chat rooms.
ISAKMP	Internet Security Association and Key Management Protocol.
ITU	International Telecommunication Union.
IUA	Individual user authentication.
JTAPI	Java TAPI.
KDC	Key Distribution Center.
laddr	Local address—The address of a host on a protected interface.
LFC	Logical Firewall Interface (as opposed to a VLAN).
LSA	link-state advertisement.
L2TP	Layer 2 Tunneling Protocol.
MGCP	Media Gateway Control Protocol.
MD5	Message Digest 5—An encryption standard for encrypting VPN packets. This same encryption is used with the **aaa authentication console** command to encrypt Telnet sessions to the console.
MIB	Management Information Base—Used with SNMP.
MPPE	Microsoft Point-To-Point Encryption.
MS-CHAP	Microsoft CHAP (Challenge Handshake Authentication Protocol). See “CHAP” for more information.
MSRPC	Microsoft Remote Procedure Call.
MTU	maximum transmission unit—The maximum number of bytes in a packet that can flow efficiently across the network with the best response time. For Ethernet, the default MTU is 1500 bytes, but each network can have different values, with serial connections having the smallest values. The MTU is described in RFC 1191.
NAT	Network Address Translation.
NBMA	nonbroadcast multiaccess.
NetBIOS	Network Basic Input Output System—An application programming interface (API) that provides special functions for PCs in LANs.

Table A-1 Acronyms and Abbreviations (continued)

Acronym	Description
NFS	Network File System.
NIC	Network Information Center.
NNTP	Network News Transfer Protocol—News reader service.
NOS	Network Operating System.
NP	IBM Network Processor.
NSSA	not so stubby area.
NTP	Network Time Protocol—Protocol that sets system clocks through the network.
NVT	Network virtual terminal.
OSPF	Open Shortest Path First protocol.
PAP	Password Authentication Protocol. Authentication protocol that lets PPP peers authenticate one another.
PAT	Port Address Translation.
PCP	Payload Compression Protocol. This is a compression protocol supplied with the Cisco IOS software code on which the FWSM IPSec implementation is based. The FWSM does not support the PCP protocol.
PDM	PIX Device Manager.
PFS	perfect forward secrecy.
PIM	Protocol Independent Multicast.
PIM-SM	PIM sparse mode.
PIX	Private Internet Exchange.
PKI	Public Key Infrastructure.
POP	Post Office Protocol.
PPPoE	Point-to-Point Protocol over Ethernet.
PPP	Point-to-Point Protocol. Provides FWSM-to-router and host-to-network connections over synchronous and asychronous circuits.
PPTP	Point-to-Point Tunneling Protocol. RFC 2637 describes the PPTP protocol.
RA	registration authority.
RADIUS	Remote Authentication Dial-In User Service—User authentication server specified with the **aaa-server** command.
RAS	The registration, admission, and status protocol. Provided with H.323 support.
RC4	RC4 is stream cipher designed by Rivest for RSA Data Security, Inc. It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation.
RFC	Request For Comment—RFCs are the defacto standards of networking protocols.
RIP	Routing Information Protocol.
RME	resource management environment.
RPC	Remote Procedure Call.
RSA	Rivest, Shamir, and Adelman. RSA is the trade name for RSA Data Security, Inc.

Table A-1 Acronyms and Abbreviations (continued)

Acronym	Description
RTP	Real-Time Transport Protocol.
RTCP	RTP Control Protocol.
RTSP	Real Time Streaming Protocol.
SA	security association.
SCCP	Simple (Skinny) Client Control Protocol.
SDP	Session Description Protocol.
SIP	Session Initiation Protocol.
SSH	Secure Shell.
SMR	Stub Multicast Routing.
SMTP	Simple Mail Transfer Protocol—Mail service. The **fixup protocol smtp** command enables the Mail Guard feature. The FWSM Mail Guard feature is compliant with both the RFC 1651 HELO and RFC 821 section 4.5.1 commands.
SNMP	Simple Network Management Protocol—Set attributes with the **snmp-server** command.
SPC	Shared Profile Component.
SPI	Security Parameter Index—A number which, together with a destination IP address and security protocol, uniquely identifies a particular security association.
SQL*Net	SQL*Net is a protocol that Oracle uses to communicate between client and server processes. (SQL stands for Structured Query Language.)
SUA	Secure unit authentication.
SYN	Synchronize sequence numbers flag in the TCP header.
TACACS+	Terminal Access Controller Access Control System Plus.
TAPI	Telephony Application Programming Interface.
TCP	Transmission Control Protocol. Refer to RFC 793 for more information.
TSE	Tree Search Engine.
TSP	TAPI Service Provider.
TFTP	Trivial File Transfer Protocol.
Triple DES	Triple Data Encryption Standard. Also known as 3DES.
TurboACL	Turbo Access Control List.
uauth	User authentication.
UDP	User Datagram Protocol.
URL	Universal Resource Locator.
UUIE	user-user information element.
VLAN	virtual LAN.
VoIP	Voice over IP.
VPDN	virtual private dial-up network.
VPN	Virtual Private Network.

Table A-1 Acronyms and Abbreviations (continued)

Acronym	Description
VTP	VLAN Trunking Protocol.
WINS	Windows Internet Name Service.
WWW	World Wide Web.
Xauth	extended authentication.
XDMCP	X Display Manager Control Protocol.
xlate	Translation slot in the FWSM.

Port and Protocol Values

This appendix lists the port and protocol values used by the FWSM and contains these sections:

Specifying Port Values

You can use literal names instead of numerical port values in command syntax.

The FWSM permits the following TCP literal names: **bgp**, **chargen**, **cmd**, **citrix-ica**, **daytime**, **discard**, **domain**, **echo**, **exec**, **finger**, **ftp**, **ftp-data**, **gopher**, **h323**, **hostname**, **http**, **ident**, **irc**, **klogin**, **kshell**, **lpd**, **nntp**, **pop2**, **pop3**, **pptp**, **rpc**, **smtp**, **sqlnet**, **sunrpc, tacacs, talk, telnet, time, uucp, whois,** and **www**.

The FWSM uses port 1521 for SQL*Net. This is the default port used by Oracle for SQL*Net; however, this value does not agree with IANA port assignments.

The FWSM listens for RADIUS on ports 1645 and 1646. If your RADIUS server uses ports 1812 and 1813, you will need to reconfigure it to listen on ports 1645 and 1646.

To assign a port for DNS access, use **domain**, not **dns**. The **dns** keyword translates into the port value for **dnsix**.

Note The FWSM drops DNS packets sent to UDP port 53 (usually used for DNS) that have a packet size larger than 512 bytes.

Permitted UDP literal names are **biff**, **bootpc**, **bootps**, **discard**, **dnsix**, **echo**, **mobile-ip**, **nameserver**, **netbios-dgm**, **netbios-ns**, **ntp**, **rip**, **snmp**, **snmptrap**, **sunrpc**, **syslog**, **tacacs**, **talk**, **tftp**, **time**, **who**, and **xdmcp**.

You can view port numbers online at this URL:

http://www.iana.org/assignments/port-numbers

Table B-1 lists the port values and literal names.

Table B-1 Port Values and Literal Names

Literal	Value	Description
administratively-prohibited	93	
alternate-address	102	
aol	60	America Online
bgp	179	Border Gateway Protocol, RFC 1163
biff	512	Used by mail system to notify users that new mail is received
bootpc	68	Bootstrap Protocol Client
bootps	67	Bootstrap Protocol Server
chargen	19	Character Generator
citrix-ica	1494	Citrix Independent Computing Architecture (ICA) protocol
cmd	514	Similar to **exec** except that **cmd** has automatic authentication
conversion-error	120	
ctiqbe	14	
daytime	13	Day time, RFC 867
discard	9	Discard
DHCP server	67	
DHCP client	68	
dod-host-prohibited	92	
dod-net-prohibited	91	
domain	53	DNS (Domain Name System)
dnsix	195	DNSIX Session Management Module Audit Redirector
echo	7, 103	Echo
echo-reply	78	Echo reply
exec	512	Remote process execution
finger	79	Finger
ftp	21	File Transfer Protocol (control port)
ftp-data	20	File Transfer Protocol (data port)
general-parameter	110	
gopher	70	Gopher
h323	1720	H.323 call signaling
host-isolated	90	
hostname	101	NIC Host Name Server
host-precedence-unreachable	94	
host-tos-unreachable	89	
host-redirect		
host-tos-redirect	101	
host-unknown	87	

Table B-1 Port Values and Literal Names (continued)

Literal	Value	Description
host-unreachable	81	
https	62	
ident	113	Ident authentication service
imap4	63	
information-reply	116	
information-request	117	
irc	194	Internet Relay Chat protocol
isakmp	500	ISAKMP
kerberos	64	
klogin	543	KLOGIN
kshell	544	Korn Shell
ldap	65	
ldaps	66	
lpd	515	Line Printer Daemon–printer spooler
login	513	Remote login
lotusnotes	67	
mask-reply	118	
mask-request	117	
mobile-ip	434	Mobile IP-Agent
mobile-redirect	121	
nameserver	42	Host Name Server
netbios-dgm	138	NETBIOS Datagram Service
net-redirect	98	
net-tos-redirect	100	
net-tos-unreachable	88	
network-unknown	86	
nntp	119	Network News Transfer Protocol
netbios-ns	137	NETBIOS Name Service
netbios-ssn	68	Network Basic Input Output System
netreachable	80	
no-room-for-option	112	
ntp	123	Network Time Protocol
option-missing	111	
packet-too-big	84	
pcanywhere-data	69	
parameter-problem	109	

Table B-1 Port Values and Literal Names (continued)

Literal	Value	Description
pcanywhere-status	73	
pim-auto-rp	496	Protocol Independent Multicast, reverse path flooding, dense mode
pop2	109	Post Office Protocol—Version 2
pop3	110	Post Office Protocol—Version 3
port-unreachable	83	Port cannot be found
pptp	70	Point-to-Point Tunneling Protocol. RFC 2637 describes the PPTP protocol
precedence-unreachable	95	Precedence cannot be found
protocol-unreachable	82	Protocol cannot be found
radius	74, 1645, 1646	Remote Authentication Dial-In User Service
radius-acct	75	Remote Authentication Dial-In User Service
reassembly-timeout	108	Specifies the timeout for reassembly
redirect	97	Redirect
router-advertisement	104	Router sends advertisement
router-solicitation	105	Queries the router
rip	520	Routing Information Protocol
rpc	71	Remote Procedure Call
secureid-udp	76	Specifies UDP secure ID
sip	58	Session Initiation Protocol
skinny	59	Simple (Skinny) Client Control Protocol
smtp	25	Simple Mail Transport Protocol
snmp	161	Simple Network Management Protocol
snmptrap	162	Simple Network Management Protocol—Trap
source-route-failed	85	Route inactive
source-quench	96	Remove sourcing
sqlnet	1521	Structured Query Language Network
ssh	72	Secure shell
sunrpc	111	Sun RPC (Remote Procedure Call)
syslog	514	System Log
tacacs	49	TACACS+ (Terminal Access Controller Access Control System Plus)
talk	517	Talk
telnet	23	RFC 854 Telnet
tftp	69	Trivial File Transfer Protocol

Table B-1 Port Values and Literal Names (continued)

Literal	Value	Description
time	37	Time
time-exceeded	106	Time exceeded
timestamp-reply	114	Returns the time stamp
timestamp-request	113	Requests a time stamp
traceroute	119	Specifies trace routing
ttl-exceeded	107	TTL is exceeded
unreachable	79	Connection refused or inactive
uucp	540	UNIX-to-UNIX Copy Program
who	513	Who
whois	43	Who Is
www	80	World Wide Web
xdmcp	177	X Display Manager Control Protocol, used to communicate between X terminals and workstations running UNIX

Specifying Protocol Values

You can specify protocols by numeric and literal values. Possible literal values are **ahp**, **eigrp**, **esp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **ipsec**, **nos**, **ospf**, **pcp**, **snp**, **tcp**, and **udp**.

You can view protocol numbers at this URL:

http://www.iana.org/assignments/port-numbers

Note Many routing protocols use multicast packets to transmit their data. If you send routing protocols across the FWSM, configure the surrounding routers with the Cisco IOS software **neighbor** command. If routes on an unprotected interface are corrupted, the routes that are transmitted to the protected side of the firewall will corrupt routers there.

Table B-2 lists the numeric values and literal names for the protocols.

Table B-2 Protocol Numeric and Literal Values

Literal	Value	Description
ah	51	Authentication Header for IPv6, RFC 1826
eigrp	88	Enhanced Interior Gateway Routing Protocol
esp	50	Encapsulated Security Payload for IPv6, RFC 1827
gre	47	General Routing Encapsulation
icmp	1	Internet Control Message Protocol, RFC 792
igmp	2	Internet Group Management Protocol, RFC 1112
igrp	9	Interior Gateway Routing Protocol
ip	0	Internet Protocol

Table B-2 Protocol Numeric and Literal Values (continued)

Literal	Value	Description
ipinip	4	IP-in-IP encapsulation
nos	94	Network Operating System (Novell's NetWare)
ospf	89	Open Shortest Path First routing protocol, RFC 1247
pcp	108	Payload Compression Protocol
snp	109	Sitara Networks Protocol
tcp	6	Transmission Control Protocol, RFC 793
udp	17	User Datagram Protocol, RFC 768

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X