

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

<i>ext_interface_name</i>	(Optional) Name of the external network where you use these global addresses.
<i>nat_id</i>	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.
<i>global_ip</i>	Global IP addresses that the FWSM shares among its connections.
<i>-global_ip</i>	(Optional) Secondary global IP address.
netmask <i>global_mask</i>	(Optional) Specifies the network mask for the <i>global_ip</i> .
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

<i>command</i>	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 hostname in the FWSM command line prompt, use the **hostname** command.

hostname *name*

Syntax Description

<i>name</i>	The hostname for the FWSM displayed in the FWSM prompt; this name can have up to 63 characters. A hostname must start and end with a letter or digit, and have as interior characters only letters, digits, or a hyphen.
-------------	--

Defaults

The default is FWSM.

Command Modes

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 hostname label on prompts.



Note

Changing the hostname 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 hostname:

```
fwsm(config)# hostname spinner
spinner(config)# hostname fws
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		
<i>ip_address</i>	Host or network authorized to initiate an HTTP connection to the FWSM.	
<i>netmask</i>	(Optional) Network mask for the http ip_address .	
<i>interface_name</i>	(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.
<i>ip_address</i>	IP address of the host sending ICMP messages to the interface.
<i>net_mask</i>	Mask to be applied to <i>ip_address</i> .
<i>icmp_type</i>	(Optional) ICMP message type as described in Table 2-9 .
<i>interface_name</i>	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 ping to an interface, and the **icmp permit** command allows you to enable ping to an interface. With ping 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:

```
fws(config)# interface inside
fws(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

<i>ip_address</i>	FWSM module's network interface IP address.
<i>mask</i>	(Optional) Network mask of <i>ip_address</i> .
standby	(Optional) Specifies the secondary or failover peer module.
<i>sby_ip_addr</i>	(Optional) IP address for the failover module.
<i>interface_name</i>	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		
	<i>poolname</i>	FWSM module's network interface IP address.
	<i>ip1</i>	IP address of the first local address pool.
	<i>-ip2</i>	(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

<i>list-name</i>	Specifies the IP prefix list name.
seq <i>seq-value</i>	(Optional) Specifies the sequence value; valid values are from 1 to 2147483646.
permit	(Optional) Permits the prefix list.
deny	Denies the prefix list.
<i>prefix/len</i>	Specifies the prefix list and prefix list length.
ge <i>min-value</i>	(Optional) Minimum length value.
le <i>max-value</i>	(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 <i>int_name</i>	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 <i>pool-name</i>	Specifies the name of a local address pool to allocate the dynamic client IP.
<i>interface-name</i>	(Optional) Name of the interface on which to enable ISAKMP negotiation.
enable <i>interface-name</i>	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 <i>seconds</i>	Specifies the keepalive interval; valid values are from 10 and 3600 seconds.
<i>retry_seconds</i>	(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 <i>keystring</i>	Specifies the authentication preshared key.
address <i>peer-address</i>	Specifies the IPsec peer's IP address for the preshared key.
netmask <i>mask</i>	(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 <i>fqdn</i>	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

<i>priority</i>	Priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
authentication <i>pre-share</i>	Specifies the preshared keys that are the authentication method.
authentication <i>rsa-sig</i>	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 <i>seconds</i>	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	<i>telnet_id</i> 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 <i>number</i> per second.	
<i>resource_name</i>	Name of the resource that you want to limit.	
all	Sets the limits for many resources, including resources that cannot be set individually.	
<i>number</i>	Number that is greater than or equal to 0.	
<i>number %</i>	(Optional) Percentage of resource limitations when used with the <i>number</i> 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:

```
fws(config-class)# class gold
fws(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.	
<i>level</i>	(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 <i>secs</i>	(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<br>Access Location: system and context command line<br>Command Mode: configuration mode<br>Firewall Mode: Routed |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|

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

| Usage Guidelines | The <b>show router ospf</b> command allows you to display the configured <b>router ospf</b> subcommands. The <b>show ip ospf</b> displays other details for the OSPF processes running. The <b>log-adj-changes</b> subcommand is enabled by default. |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

| Examples | This example shows how to enable system log messages: |
|----------|-------------------------------------------------------|
|----------|-------------------------------------------------------|

```
fwm(config)# router ospf 1
fwm(config-router)# log-adj-changes detail
fwm(config-router)#
```

| Related Commands | <a href="#">router ospf</a><br><a href="#">show log-adj-changes</a><br><a href="#">show ip ospf</a><br><a href="#">show router ospf</a> |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------|

# 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

|                                 |                                                                                                                                                                               |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>on</b>                       | Sends syslog messages to all output locations.                                                                                                                                |
| <b>buffered level</b>           | Sends the specified syslog level messages to an internal buffer that can be viewed with the <b>show logging</b> command; see the “Usage Guidelines” section for valid values. |
| <b>console level</b>            | Specifies that the specified syslog level messages appear on the FWSM console as each message occurs; see the “Usage Guidelines” section for valid values.                    |
| <b>facility facility</b>        | Specifies the syslog facility; valid values are <b>16</b> (LOCAL0) through <b>23</b> (LOCAL7).                                                                                |
| <b>history level</b>            | Specifies the SNMP message level for sending syslog traps; see the “Usage Guidelines” section for valid values.                                                               |
| <b>message syslog_id</b>        | Specifies a message number to disallow or allow.                                                                                                                              |
| <b>level level</b>              | (Optional) Specifies the syslog message level as a number or string; see the “Usage Guidelines” section for valid values.                                                     |
| <b>monitor level</b>            | Specifies that the syslog messages appear on Telnet sessions to the FWSM console; see the “Usage Guidelines” section for valid values.                                        |
| <b>queue queue_size</b>         | Specifies the size of the queue for storing syslog messages. The <i>queue_size</i> length limit of the log queue is 0, unlimited..                                            |
| <b>standby</b>                  | Allows the failover standby module to send syslog messages.                                                                                                                   |
| <b>timestamp</b>                | Specifies that syslog messages that are sent to the syslog server should have a time-stamp value on each message.                                                             |
| <b>trap level</b>               | Specifies the logging level for syslog messages only.                                                                                                                         |
| <b>device-id</b>                | Specifies that the device ID of the FWSM is included in the syslog message.                                                                                                   |
| <b>hostname</b>                 | Specifies to use the host name of the FWSM to uniquely identify the syslog messages from the FWSM.                                                                            |
| <b>ipaddress interface_name</b> | Specifies to use the IP address of the specified FWSM interface to uniquely identify the syslog messages from the FWSM.                                                       |
| <b>string text</b>              | Specifies the text string to uniquely identify the syslog messages from the FWSM.                                                                                             |
| <b>context-name</b>             | Specifies the context.                                                                                                                                                        |
| <b>host</b>                     | Specifies a syslog server that will receive the messages that are sent from the FWSM.                                                                                         |
| <i>in_intf</i>                  | Interface on which the syslog server resides.                                                                                                                                 |

|                          |                                                                                                                                                                                                                                                  |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>syslog_ip</i>         | Syslog server's IP address.                                                                                                                                                                                                                      |
| <i>port</i>              | (Optional) Port from which the FWSM sends either UDP or TCP syslog messages; valid values are as follows: <ul style="list-style-type: none"> <li>• The UDP port is from 1025 to 65535.</li> <li>• The TCP port is from 1025 to 65535.</li> </ul> |
| <b>format emblem</b>     | (Optional) Enables EMBLEM format logging for each syslog server.                                                                                                                                                                                 |
| <b>interface</b>         | (Optional) Specifies that only the messages that are associated with those interfaces listed are sent to the host.                                                                                                                               |
| <i>if1 [if2] ... ]</i>   | Specifies the interface.                                                                                                                                                                                                                         |
| <b>buffer-size bytes</b> | 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](#)  
[show logging](#)  
[show logging rate-limit](#)

# logging rate-limit

To limit the rate at which the syslog message 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

|                                  |                                                                                                                                                                                                                                                                                  |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>unlimited</b>                 | Disables rate limiting.                                                                                                                                                                                                                                                          |
| <i>num</i>                       | Number at which the syslog message is to be rate limited.                                                                                                                                                                                                                        |
| <i>interval</i>                  | (Optional) Time interval (in seconds) during which the syslogs should be limited.                                                                                                                                                                                                |
| <b>message</b>                   | Suppresses reporting of this syslog message.                                                                                                                                                                                                                                     |
| <i>syslog_id</i>                 | ID of the syslog message to suppress reporting.                                                                                                                                                                                                                                  |
| <b>level</b> <i>syslog_level</i> | Applies the set rate limits on all system log messages that belong to a certain syslog message suppression level. All system log messages at a specified syslog message suppression level are rate-limited individually. The valid range for <i>syslog_level</i> is 1 through 7. |

## 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**

To limit the rate of syslog message generation, you can enter a specific message ID. The following example shows how to limit the rate of system log message generation using a specific message ID and time interval:

```
fws(config)# logging rate-limit 100 600 message 302020
```

This example suppresses system log message 302020 from being sent to the host after the rate limit of 100 is reached in the specified interval of 600 seconds.

To limit the rate of system log message generation, you can enter a specific syslog message suppression level. The following example shows how to limit the rate of system log message generation using a specific syslog message suppression level and time interval.

```
fws(config)# logging rate-limit 100 600 level 6
```

This example suppresses all system log messages under syslog message suppression level 6 to the specified rate limit of 1000 in the specified time interval of 600 seconds. Each system log message in syslog message suppression level 6 has a rate limit of 1000.

---

**Related Commands**

[clear logging](#)  
[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:

```
fws> 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](#)