

same-security-traffic permit inter-interface

To enable the same-security level interface communication, use the **same-security-traffic permit inter-interface** command. To disable the same-security interfaces, use the **no** form of this command.

[no] same-security-traffic permit inter-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: 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) # same-security-traffic permit inter-interface
```

Related Commands [clear 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 metric-type { type-1 | type-2 | internal | external } ip next-hop
ip-address [ip-address]
```

Syntax Description		
metric		Specifies metric values.
+ or -		(Optional) Specifies positive or negative metric values.
<i>metric_value</i>		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 next-hop		Specifies where to send packets that pass a match clause of a route map.
<i>ip-address</i>		Specifies the IP address of the next hop to which to output packets.
<i>ip-address</i>		(Optional) Specifies the 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.

Usage Guidelines The *ip_address* must be the address of an adjacent router.

Examples This example shows how to send packets passed by a match clause of a route map:

```
fws(config-route-map) # set ip next-hop 123.24.30.10
```

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 ip next-hop (route map submode)

To specify where to send packets that pass a match clause of a route map, use the **set ip next-hop** subcommand. To delete an entry, use the **no** form of this command.

set ip next-hop *ip-address* [*ip-address*]

no set ip next-hop *ip-address*

Syntax Description		
	<i>ip-address</i>	Specifies the IP address of the next hop to which to output packets.
	<i>ip-address</i>	(Optional) Specifies the IP address of the secondary next hop.

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 firewall mode

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

Usage Guidelines The *ip_address* must be the address of an adjacent router.

Examples This example shows how to send packets passed by a match clause of a route map:

```
fwsM/context_name(config)# set ip next-hop 123.24.30.10
```

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:

```
fws(config)# route-map maptag1 permit 8
fws(config-route-map)# set metric 5
fws(config-route-map)# match metric 5
fws(config-route-map)# set metric-type type-2
fws(config-route-map)# show route-map
route-map maptag1 permit 8
    set metric 5
    set metric-type type-2
    match metric 5
fws(config-route-map)# exit
fws(config)#
```

■ **set metric (route map submode)**

Related Commands

- [match \(route map submode\)](#)
- [route-map](#)
- [set ip next-hop \(route map submode\)](#)
- [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:

```
fws(config)# route-map maptag1 permit 8
fws(config-route-map)# set metric 5
fws(config-route-map)# match metric 5
fws(config-route-map)# set metric-type type-2
fws(config-route-map)# show route-map
route-map maptag1 permit 8
    set metric 5
    set metric-type type-2
    match metric 5
fws(config-route-map)# exit
fws(config)#
```

Related Commands

- route-map
- set ip next-hop (route map submode)

■ **set metric-type (route map submode)**

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 2-13](#).

Table 2-13 FWSM Setup Information

Prompt	Description
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.
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.

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:

```
fws(config)# setup
Pre-configure FWSM Firewall now through interactive prompts [yes]? y
Enable Password [<use current password>]: ciscofws
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: accounting_fws
Domain name: example.com
IP address of host running FWSM Device Manager: 192.168.1.2
```

The following configuration will be used:

```
Enable Password: ciscofws
Clock (UTC): 22:47:37 Sep 12 2001
Inside IP address: ...192.168.1.1
Inside network mask: ...255.255.255.0
Host name: ...accounting_fws
Domain name: ...example.com
IP address of host running Device Manager: ...192.168.1.2
```

Use this configuration and write to flash? **y**

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

<i>command_keywords</i>	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) Specifies verbose mode.
<i>regexp</i>	(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: 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 *regex* 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.
dhcpcd       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 interface
interface	Set network interface parameters 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

■ show

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: 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 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: 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: 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 display the context group members, use the **show access-group** command.

show access-group [*access-list*]

Syntax Description	<i>access-list</i> (Optional) Access list <i>id</i> .
---------------------------	---

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.

Examples	This example shows how to display the context group members:
-----------------	--

```
fwsM/context_name(config)# show access-group
access-group 100 in interface outside
```

Related Commands	access-group
-------------------------	---------------------

show access-list

To display the access list entries by number, use the **show access-list** command.

show access-list *id*

Syntax Description	<i>id</i>	Identifies the 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: 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 numbers the access list entries (ACEs) and remarks are inserted. The remarks are not assigned a line number.

```
fws(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)
```

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: 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 display the access list compilation mode for the FWSM:

```
fws(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: 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:

```
fws(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.
fws(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: 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.

Examples This example shows how to display the designated administration context:

```
fws(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: 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 alias information:

```
fwsM/context_name(config)# show alias
```

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: 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
 Access Location: system command line
 Command Mode: 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 list the entries in the ARP table:

```
fws(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: 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: 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

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 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.

Syslog messages 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 2-14 describes the columns in the **show blocks** display.

Table 2-14 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 2-15 describes the rows in the **show blocks** display.

Table 2-15 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:

```
fwsn(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
```

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 2-16 describes strings within the **show ca certificate** command sample output.

Table 2-16 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 2-16 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 2-16](#) for descriptions of the strings within the following sample output.

```
fwsd(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.

```
fwsd(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 display a certificate with a CRL string. See [Table 2-16](#) for descriptions of the strings within the following sample output.

```
fwsd(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 [capture_name] [access-list access_list_name] [count number] [detail] [dump]
```

Syntax Description

<i>capture_name</i>	(Optional) Name of the packet capture.
access-list <i>access_list_name</i>	(Optional) Displays information for packets that are based on IP or higher fields for the specific access list identification.
count <i>number</i>	(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: 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 2-17](#), the bracketed output is displayed when you specify the **detail** keyword.

Table 2-17 Packet Capture Output Formats

Packet Type	Capture Output Format
802.1Q	<i>HH:MM:SS.ms</i> [ether-hdr] <i>VLAN-info</i> <i>encap-ether-packet</i>
ARP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>arp-type</i> <i>arp-info</i>
IP/ICMP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>ip-source</i> > <i>ip-destination</i> : icmp: <i>icmp-type</i> <i>icmp-code</i> [checksum-failure]
IP/UDP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>src-addr.src-port</i> <i>dest-addr.dst-port</i> : [checksum-info] <i>udp</i> <i>payload-len</i>

Table 2-17 Packet Capture Output Formats (continued)

Packet Type	Capture Output Format
IP/TCP	<i>HH:MM:SS.ms</i> [ether-hdr] <i>src-addr.src-port dest-addr.dst-port: tcp-flags</i> [header-check] [checksum-info] <i>sequence-number ack-number tcp-window urgent-info tcp-options</i>
IP/Other	<i>HH:MM:SS.ms</i> [ether-hdr] <i>src-addr dest-addr: ip-protocol ip-length</i>
Other	<i>HH:MM:SS.ms ether-hdr: hex-dump</i>

Examples

This example shows how to display the capture configuration:

```
fws(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:

```
fws(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: 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:

```
fws(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: 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:

```
fws(config)# show class
Class Name      Members      ID   Flags
default         All          1    0001
fws(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: 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: 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:

```
fswm/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: 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][,...]]
```

Syntax Description

count	(Optional) Displays only the number of used connections.
protocol TCP	(Optional) Displays active TCP connections; see the “Usage Guidelines” section for additional information.
protocol UDP	(Optional) Displays active UDP connections; see the “Usage Guidelines” section for additional information.
protocol icmp	(Optional) Displays active ICMP connections; see the “Usage Guidelines” section for additional information.
foreign ip -ip2	(Optional) Displays active connections by the foreign IP address.
local ip -ip2	(Optional) Displays 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 active connections by their current state; see the “Usage Guidelines” section for additional information.
<i>up</i>	(Optional) Displays active connections.
<i>,finin</i>	(Optional) Displays the foreign connection state in.
<i>,finout</i>	(Optional) Displays the foreign connection state out.
<i>,http_get</i>	(Optional) Displays the HTTP connection state.
<i>,smtp_data</i>	(Optional) Displays the SMTP connection state.
<i>,data_in</i>	(Optional) Displays the data connection state.
<i>,data_out</i>	(Optional) Displays the data connection state out.
<i>,...</i>	(Optional) Displays other connections.

Command Modes

Security Context Mode: single context mode and multiple context mode

Access Location: system 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 **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:

```
fws(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 2-18](#).

Table 2-18 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 2-18 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.

```
fws(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.

```
fws(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
```

show conn

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: 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:

```
fws(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.
	<i>name</i>	(Optional) Displays 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: 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.
<i>context-name</i>	(Optional) Specifies the context name.
top <i>N</i>	(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.
<i>protocol_name</i>	(Optional) Specifies a protocol by name.
: <i>counter_name</i>	(Optional) Specifies a counter by name.
detail	(Optional) Displays the counters in detail.
threshold	(Optional) Displays only those counters at or above the specified threshold.
<i>count_threshold</i>	(Optional) Specifies the 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: 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
```

show counters

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:

```
fws# 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:

```
fws# 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.
<i>context_name</i>	(Optional) Specifies a 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: 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%. 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:

```
fws(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:

```
fws/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:

```
fws(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: 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:

```
fws(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.)

```
fws(config)# crashdump test
fws(config)# exit
fws(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 @ 0xffffd8000, 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

```

■ show crashdump

```

.
.
.
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 (Optional) Shows the crypto dynamic map set with the specified <i>map-name</i> . <i>dynamic-map-name</i>
---------------------------	--

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 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
```

show crypto dynamic-map

```
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”:

```
fwsn(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 or run the Known Answer Test (KAT), use the **show crypto engine** command.

show crypto engine [verify]

Syntax Description

verify (Optional) Runs the Known Answer Test (KAT).

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:

```
fws(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 2-19](#)) for the FWSM VAC+ only.

Table 2-19 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 2-19 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	5 second, 1 minute, and 5 minute moving averages of the packet count and payload bytes through all crypto interface cards.
5second	
1minute	
5minute	

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
```

show crypto interface

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+):

```
fws(config)# show crypto interface
fws(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 <i>transform-set-name</i>	(Optional) Specifies a transform set.
sa	Displays the settings that are used by the current security associations.
map <i>map-name</i>	(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: 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	Parameter	Description
	interface <i>interface-name</i>	(Optional) Displays the identifying interface to be used by the FWSM to identify itself to peers.
	tag <i>map-name</i>	(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: 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: 010203040506070809010203040506070809010203040506070809,
Outbound esp spi: 0
  cipher key: ,
  auth key: ,
Outbound ah spi: 256,
  key: 010203040506070809010203040506070809010203040506070809,
```

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
010203040506070809010203040506070809010203040506070809
fwsM/context_name(config)# crypto map multi-peer 20 set session-key outbound ah 256
010203040506070809010203040506070809010203040506070809
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.

```
fws(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
fws(config)# exit
```

```
fws(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
fws(config)# exit
```

```
fws(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
fws(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: 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 (route 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: 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:

```
fws(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 **dbg**

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: 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:

```
fws(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: 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: 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 | fileys

Syntax Description	all	Displays all files in the file system and the geometry of the partitions.
	fileys	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: 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:

```
fwsd(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:

```
fwsd(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:

```
fws(config)# show disk filesystems

***** 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: 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 :              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 connection :          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: 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	xmcp	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	xmcp	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: 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:

```
fws(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: 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: 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 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: 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: 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: 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 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.

Examples

This example shows how to display failover information:

```
fwsd(config)# show failover
Failover Off
Failover unit Secondary
Failover LAN Interface not Configured
Unit Poll frequency 1 seconds
Interface Poll frequency 15 seconds
Interface Policy 50%
Monitored Interfaces 0 of 250 maximum
```

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: 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:

```
fws(config)# show file descriptors
No open file descriptors
fws(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
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: 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: 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:

```
fws(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: 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:

```
fwsn(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:

```
fws(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: 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**
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: 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	<i>interface</i> (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: 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:

```
fwsn(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: 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:

```
fws(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: 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:

```
fws(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: 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: 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: 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: 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 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: 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: 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

<i>group</i>	(Optional) Address of the multicast group to join.
interface <i>interface_name</i>	(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:

```
fws(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: 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**
- 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	
<i>interface</i>	(Optional) Identifies the 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: 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:

```
fwsd(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 nameif'd, but shut
vlan41 - trunked and nameif'd, but the vlan has been shut from system.
fws(config)#

```

This example shows how to display the interface statistics:

```

fws(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	<i>interface_name</i> (Optional) Specifies an 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: 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:
-----------------	--

```
fwsd(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	
	<i>pid</i> (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: 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:

```
fws(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
fws(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 DChitless 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 submenu)
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: 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

<i>pid</i>	(Optional) ID of the OSPF process.
database	Displays the database information.
internal	(Optional) Routes that are internal to a specified autonomous system.
adv-router	(Optional) Advertised router.
<i>addr</i>	(Optional) Router address.
<i>area_id</i>	(Optional) ID of the area that is associated with the OSPF address range.
self-originate	(Optional) Displays the information for the specified autonomous system.
<i>lsid</i>	(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 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: 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	<i>interface_name</i>	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: 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: <pre>fwsm/context_name(config)# show ip ospf flood-list outside</pre>
----------	---

Related Commands	<pre>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</pre>
------------------	--

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	
<i>interface_name</i>	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: 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	
<i>interface_name</i>	(Optional) Name of the interface for which to display neighbor information.
<i>nbr_router_id</i>	(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: 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	<i>nbr_router_id</i>	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.
	<i>interface_name</i>	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: 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	<i>nbr_router_id</i>	ID of the neighbor router that is specified by its IP address.
	<i>interface_name</i>	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: 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: 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: 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 <i>int_name</i>	(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: 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:

```
fws(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: 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 2-20](#) lists the descriptions for the **show isakmp sa detail** command output.

Table 2-20 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 2-20 *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 the **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: 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	
<i>ip_address</i>	(Optional) Specifies the 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: 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 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:

```
fwsn/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: 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:
-----------------	---

```
fws(config)# show log-adj-changes
```

Related Commands	log-adj-changes 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.
<i>syslog_id</i>	Specifies a 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: 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:

```
fws(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 **fws-1**:

```
fws(config)# logging device-id hostname
fws(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 "fws-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: 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-table

To display the information about the MAC-address table, use the **show mac-address-table** command.

show mac-address-table [static]

Syntax Description	static (Optional) Displays the static MAC addresses in the bridge table.
---------------------------	---

Command Modes	Security Context Mode: single context mode and multiple context mode Access Location: context command line Command Mode: 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: <pre>fws(config)# show mac-address-table</pre>
-----------------	--

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: 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:

```
fwsn(config)# show mac-learn
```

Related Commands **clear mac-learn**
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:

```
fws(config)# show match
```

Related Commands

- match (route map submenu)**
- match interface (route map submenu)**
- match ip next-hop (route map submenu)**
- match route-type (route map submenu)**
- 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: 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:

```
fws(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:

```
fwm/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
```

show mgcp

```
fwsn/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: 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 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. Interfaces must be configured before you use this command to receive information from this command.

Examples This example shows how to display information about the monitored interface:

```
fwsM/context_name(config)# show monitor-interface
This host:Primary - Active
    Interface mgmt (10.7.1.1):Normal
    Interface inside (20.8.1.1):Normal
Other host:Secondary - Standby
    Interface mgmt (10.7.1.2):Normal
    Interface inside (20.8.1.2):Normal
fwsM/context_name(config)#
```

Related Commands

- failover interface ip
- failover interface-policy
- failover lan interface
- monitor-interface
- 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		
	<i>dst</i>	(Optional) Displays multicast route table information that is based on the specified Class D address of the multicast group.
	<i>src</i>	(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: 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:

```
fws(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 (Optional) Displays the per-interface multicast settings. <i>interface_name</i>
---------------------------	---

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.

Examples	This example shows how to display all multicast settings:
-----------------	---

```
fwsn(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: 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.

```
fws(config)# show name
System IP Addresses:
  name 192.168.42.3 fws_inside
  name 209.165.201.3 fws_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: 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:

```
fws(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: 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: 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 UDP 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		
<i>prefix</i>		IP address.
<i>ip_address</i>		Router ID in IP address format.
<i>netmask</i>		IP address mask or IP subnet mask used for a summary route.
area <i>area_id</i>		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: 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: 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 status of the internal NICs:

```
fws(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.
<i>obj_grp_id</i>	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: 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 2-21](#) lists the descriptions for the **show object-group** commands and their accompanying configuration commands.

Table 2-21 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.

show object-group**Examples**

This example shows how to remove all the **object** commands from the configuration:

```
fws(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:

```
fws(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: 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 <i>interface_name</i>	(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 *session_id*, beginning with session number 0.

Examples

This example shows how to display the contents of the PDM history buffer:

```
fws(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:

```
fws(config)# pdm history enable
fws(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

clearn 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: 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: my_context
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
TCP Intercept       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
```

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 <i>command</i>	(Optional)	Displays the privilege level for a specific command.
level <i>level</i>	(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: 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:

```
fws(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: 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:

```
fws(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 FragDBG
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 <i>metric_value</i>	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type <i>metric_type</i>	(Optional) Specifies the OSPF metric type; valid values are type-1 , type-2 , internal , or external .
route-map <i>map_name</i>	(Optional) Name of the route map to apply.
tag <i>tag_value</i>	(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 <i>pid</i>	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 <i>type</i>	(Optional) Specifies the OSPF metric routes that are internal to a specified autonomous system; valid values are either type 1 or 2.
external <i>type</i>	(Optional) Specifies the OSPF metric routes that are external to a specified autonomous system; valid values are either type 1 or 2.
nssa-external <i>type</i>	(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: 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:

```
fws(config)# show redistribute
```

Related Commands

```
redistribute  
router ospf  
show ip ospf
```

show resource allocation

To display a list of system resource allocation, 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: 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 how to display a list of system resource allocations: The following sample display 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 2-22](#) shows each field description.

Table 2-22 show resource allocation Fields

Field	Description
Resource	The name of the resource that you can limit.
Total	The 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.

The following sample display 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%
```

show resource allocation

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 2-23 shows each field description.

Table 2-23 show resource allocation detail Fields

Field	Description
Resource	The name of the resource that you can limit.
Class	The name of each class, including the default class. The All contexts field shows the total values across all classes.
Mmbrs	The number of contexts assigned to each class.
Origin	The origin of the resource limit, as follows: <ul style="list-style-type: none"> 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.” The FWSM can combine “A” with “C” or “D.”
Limit	The 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	The 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	The 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: 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:

```
fws# 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-spec	(Optional) Specifies an internal or external network interface to display.
resource-spec	(Optional) Specifies a resource to display.
counter-spec	(Optional) Specifies a counter to display.
context	(Optional) Specifies the context.
<i>context_name</i>	(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.
<i>resource_name</i>	(Optional) Specifies a resource name
all	(Optional) Specifies all resources.
detail	(Optional) Specifies detail.
counter	(Optional) Specifies a specific resource counter.
<i>counter_name</i>	(Optional) Specifies the counter name.,
<i>count_threshold</i>	(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: 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 usage:

The following sample display shows the resource usage for all contexts and all resources.

The following sample display shows the resource usage for all contexts and all resources.

```
fws# 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.
```

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	<i>interface_name</i> (Optional) Specifies an internal or external network interface to display.
---------------------------	--

Defaults	This command has no default settings.
-----------------	---------------------------------------

Command Modes	<p>Security Context Mode: single context mode</p> <p>Access Location: system and context command line</p> <p>Command Mode: privileged mode</p> <p>Firewall Mode: Routed</p>
----------------------	---

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:
-----------------	--

```
fws(config)# show rip
rip outside passive
no rip outside default
rip inside passive
no rip inside default
```

Related Commands	<p>clear rip</p> <p>rip</p>
-------------------------	---

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		
	<i>ifc_name</i>	Server interface name.
	<i>ip_addr</i>	RPC server IP address.
	<i>mask</i>	Network mask.
	service	Specifies a service.
	<i>service_type</i>	Sets the RPC service program number as specified in the rpcinfo command.
	protocol tcp	Specifies the RPC transport protocol.
	protocol udp	Specifies the RPC transport protocol.
	port <i>port</i> [<i>- port</i>]	Specifies the RPC protocol port range.
	port- <i>port</i>	(Optional) Specifies the RPC protocol port range.
	timeout <i>hh:mm:ss</i>	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: 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:

```
fwsn(config)# show rpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout 0:03:00
```

■ show rpc-server

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	
<i>interface_name</i>	(Optional) Internal or external network interface name.
<i>ip_address</i>	(Optional) Internal or external network IP address.
<i>netmask</i>	(Optional) Network mask to apply to <i>ip_address</i> .
<i>gateway_ip</i>	(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: 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:

```
fws(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	<i>map_tag</i>	(Optional) Text for the route-map tag.
--------------------	----------------	--

Defaults	This command has no default settings.
----------	---------------------------------------

Command Modes	<p>Security Context Mode: single context mode</p> <p>Access Location: system and context command line</p> <p>Command Mode: privileged mode</p> <p>Firewall Mode: routed firewall mode</p>
---------------	---

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 show how to display a route map for use in OSPF routing:
----------	---

```
fwsn(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	<i>ip_address</i>	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: 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:

```
fwsn(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

<i>ip_address</i>	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: 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:

```
fwsms(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.
<i>interface_name</i>	(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: 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
```

■ show routing

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: 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 fwmdoc515
domain-name cisco.com
fixup protocol ftp 21
```

show running-config

```

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
```

Related Commands **clear same-security-traffic**
same-security-traffic permit inter-interface

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: 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:

```
fwsd(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
fwsd 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: 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:

```
fws(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:

```
fws(config)# show set
service resetinbound
```

Related Commands **set ip next-hop (route map submode)**
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	
<i>src_ip</i>	(Optional) Displays the address of the attacking host.
<i>statistics</i>	(Optional) Displays the 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
 Firewall 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:
 fsm/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: 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	Parameter	Description
	sessions	Displays all active SSH sessions on the FWSM.
	<i>ip_address</i>	(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: 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 2-24](#) lists the SSH states that appear in the State column:

Table 2-24 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 2-24 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:

```
fwm/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: 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:

```
fwsmdoc515(config)# show startup-config
: Saved
: Written by enable_15 at 17:14:09.092 UTC Tue Apr 9 2002
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
```

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: 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 UDP 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		
<i>addr</i>	Value of the summary address that is designated for a range of addresses.	
<i>netmask</i>	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 <i>tag_value</i>	(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: 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:

```
fwm/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: 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	
<i>url</i>	(Optional) Sends the information to a URL.
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: 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-support** 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:

```
fwsd(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 @ 0xffffd8000, 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 Collec
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	00f2bfb3	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
Crđ	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

show tech-support

```

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:

```
fwsmd(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 @ 0xffffd8000, 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 Collec
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 00f2bfb3 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
Crđ 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:0000000000000000000000000000000000000000
: 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: 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:

```
fws(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: 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 2-25](#).

Table 2-25 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_rev good pkts	Number of good packets that were received by the TCP stack.
tcp_rev 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 2-25 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
tcp_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 checksum = 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: 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: 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	<i>protocol</i> (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: 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 <i>spf_delay</i>	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 <i>spf_holdtime</i>	Hold time between two consecutive SPF calculations in seconds; valid values are from 0 to 65535.	
lsa-group-pacing <i>seconds</i>	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: 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
```

■ 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	
	<i>username</i> (Optional) Displays the user authentication information by username.

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 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:

```
fwsd(config)# show uauth
Authenticated Users      Current      Most Seen
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:

```
fwsd(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: 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: 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:
----------	---

```
fws(config)# show url-block
url-block url-mempool 128
url-block url-size 4
url-block block 128

fws(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: 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
```

■ show url-cache stat

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: 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
```

■ show url-server

```
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

<i>name</i>	Displays the 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: 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: 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:

```
fws(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: 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:

```
fws(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	<i>group_name</i> (Optional) Displays 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: 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	<i>local_ip</i> (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 **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)	Network mask to qualify the global or local IP addresses.
gport port		Display 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		Display 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.
<i>if1 ,if2</i>	(Optional)	Specifies the interface.
state	(Optional)	Displays the active translations by state.
<i>static</i>	(Optional)	Specifies the 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: 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 2-26](#).

Table 2-26 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):

```
fws(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:

```
fws(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.

```
fws(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

<i>src_ip</i>	Address of the attacking host.
<i>dst_ip</i>	(Optional) Address of the target host.
<i>src_port</i>	(Optional) Source port of the connection causing the shun.
<i>dest_port</i>	(Optional) Destination port of the connection causing the shun.
<i>protocol</i>	(Optional) IP protocol, such as UDP or TCP.
<i>vlan</i>	Specifies the 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.

```
snmp-server { community key } | { contact | location } text } | { host [interface_name] ip_addr [ trap | poll ] } | { enable traps }
```

```
no snmp-server { community | contact | location | enable traps | trap | poll }
```

Syntax Description

community <i>key</i>	Specifies the password key value at the SNMP management station.
contact <i>text</i>	Specifies the name of the contact person or the FWSM system administrator.
location <i>text</i>	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.
<i>interface_name</i>	(Optional) Interface name where the SNMP management station resides.
<i>ip_addr</i>	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.
enable traps	Enables sending log messages as SNMP trap notifications.

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.

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
```

Examples

This example shows the commands that you would enter to start receiving 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 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

<i>local_ip</i>	IP address of the host or network authorized to initiate an SSH connection to the FWSM.
<i>mask</i>	Network mask for <i>ip_address</i> . If you do not specify a <i>netmask</i> , the default is 255.255.255.255 regardless of the class of <i>ip_address</i> .
<i>interface_name</i>	(Optional) FWSM interface name on which the host or network initiating the SSH connection resides.
timeout <i>mm</i>	Specifies the duration in minutes that a session can be idle before being disconnected; valid values are from 1 to 60 minutes.
disconnect <i>session_id</i>	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 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

<i>real_ifc</i>	(Optional) Name of the network interface, as specified by the nameif command, where the hosts or networks designated by the specified <i>real_ip</i> or sources in the access list are accessed.
<i>mapped_ifc</i>	(Optional) Name of the network interface, as specified by the nameif command, where the <i>real_ip</i> argument or by the source in the access-list are translated into the <i>mapped_ip</i> argument.
<i>mapped_ip</i>	Masquerade address of the <i>real_ip</i> argument or of the source address in the access-list.
interface	Address taken from the <i>mapped_ifc</i> argument.
<i>real_ip</i>	Address as configured at the actual host.
netmask mask	Specifies the IP netmask to apply to the specified <i>real_ip</i> argument.
access-list	Allows you to identify local traffic for network address translation (NAT) by specifying the local and destination addresses (or ports).
<i>access_list_name</i>	Specifies the access list name.
dns	(Optional) Rewrites the local address in DNS replies to the global address.
norandomseq	(Optional) Disables TCP Initial Sequence Number (ISN) randomization protection.
tcp	(Optional) Specifies that maximum TCP connections and embryonic limits are set for TCP.
<i>max_conns</i>	Maximum number of simultaneous TCP connections that each <i>real_ip</i> variable host is allowed to use. Idle connections are closed after the time specified by the timeout conn command.
<i>emb_lim</i>	(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.
<i>udp_max_conns</i>	(Optional) Used with the udp keyword to set the maximum number of simultaneous UDP connections the <i>local_ip</i> hosts are each allowed to use.
tcp	Specifies TCP static PAT.
udp	Specifies UDP static PAT.
<i>mapped_ip</i>	Mapped IP address; the mapped IP address and the real IP address must be in the same network.
<i>mapped_port</i>	Masquerade port of the specified <i>real_port</i> or of the source port in the access list.

<i>real_port</i>	Specifies the 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 than 4000 static entries across all contexts.

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. Connection attempts from 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 transfer 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-ISBN 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 should 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

<i>addr</i>	Value of the summary address that is designated for a range of addresses.
<i>netmask</i>	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 <i>tag_value</i>	(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 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 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 access check.
timewait		Specifies that the TCP connections undergo the TIMEWAIT state.
tcpmss		Sets the maximum limit of the TCP MSS bytes.
minimum		Sets the minimum limit of the TCP MSS bytes.
<i>bytes</i>		Specifies the byte count for tcpmss and minimum .
zombie-timeout		Sets the zombie timeout.
<i>seconds</i>		(Optional) Specifies the zombie timeout.
nodnsalias inbound		Disables alias inbound DNS A record translation.
nodnsalias outbound		Disables alias outbound DNS A record translation.
noproxyarp		Disables proxy ARP on the specified interface.
<i>interface_name</i>		
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:

```
fwsd(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:

```
fwsd/context_name(config)# aaa-server my-aaa-server-group (inside) host 192.168.0.10 key
12345678
fwsd/context_name(config)# aaa-server my-aaa-server-group protocol radius
fwsd/context_name(config)# vpdn group 1 accept dialin pptp
fwsd/context_name(config)# vpdn group 1 ppp authentication mschap
fwsd/context_name(config)# vpdn group 1 ppp encryption mppe auto required
fwsd/context_name(config)# vpdn group 1 client configuration address local my-addr-pool
fwsd/context_name(config)# vpdn group 1 client authentication aaa my-aaa-server-group
fwsd/context_name(config)# vpdn group 1 client configuration dns 10.2.2.99
fwsd/context_name(config)# vpdn group 1 client configuration wins 10.2.2.100
fwsd/context_name(config)# vpdn enable outside
fwsd/context_name(config)# access-list nonat permit ip 10.1.1.0 255.255.255.0 host
192.168.0.2
fwsd/context_name(config)# access-list nonat permit ip 10.1.1.0 255.255.255.0 host
10.2.2.99
fwsd/context_name(config)# access-list nonat permit ip 10.1.1.0 255.255.255.0 host
10.2.2.100
fwsd/context_name(config)# nat (inside) 0 access-list nonat
fwsd/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:

```
fwsd/context_name(config)# static 172.21.100.123 172.21.100.123
fwsd/context_name(config)# access-list 10 permit ip host 172.21.200.67 host 172.21.100.123
fwsd/context_name(config)# crypto ipsec transform-set t1 esp-des esp-md5-hmac
fwsd/context_name(config)# crypto map mymap 10 ipsec-isakmp
fwsd/context_name(config)# crypto map mymap 10 match address 10
fwsd/context_name(config)# crypto map mymap 10 set transform-set t1
fwsd/context_name(config)# crypto map mymap 10 set peer 172.21.200.1
fwsd/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