



CHAPTER

22

pager through pwd Commands

pager

To set the default number of lines on a page before the “---more---” prompt appears for Telnet sessions, use the **pager** command in global configuration mode.

pager [**lines**] *lines*

Syntax Description

[lines] *lines* Sets the number of lines on a page before the “---more---” prompt appears. The default is 24 lines; 0 means no page limit. The range is 0 through 2147483647 lines. The **lines** keyword is optional and the command is the same with or without it.

Defaults

The default is 24 lines.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was changed from a privileged EXEC mode command to a global configuration mode command. The terminal pager command was added as the privileged EXEC mode command.

Usage Guidelines

This command changes the default pager line setting for Telnet sessions. If you want to temporarily change the setting only for the current session, use the **terminal pager** command.

If you Telnet to the admin context or session to the system execution space, then the pager line setting follows your session when you change to other contexts, even if the **pager** command in a given context has a different setting. To change the current pager setting, enter the **terminal pager** command with a new setting, or you can enter the **pager** command in the current context. In addition to saving a new pager setting to the context configuration, the **pager** command applies the new setting to the current Telnet session.

If there are two or more concurrent Telnet or ssh sessions, and one of the sessions is at the “---more---” (more) prompt, the other sessions cannot do anything until the more prompt is dismissed. To avoid the more prompt altogether, enter the **pager lines 0** command.

Examples

The following example changes the number of lines displayed to 20:

```
hostname(config)# pager 20
```

Related Commands

Command	Description
clear configure terminal	Clears the terminal display width setting.
show running-config terminal	Displays the current terminal settings.
terminal	Allows system log messages to display on the Telnet session.
terminal pager	Sets the number of lines to display in a Telnet session before the “---more---” prompt. This command is not saved to the configuration.
terminal width	Sets the terminal display width in global configuration mode.

passwd

To set the login password, use the **passwd** command in global configuration mode. To set the password back to the default of “cisco,” use the **no** form of this command. You are prompted for the login password when you access the CLI as the default user using Telnet or SSH. After you enter the login password, you are in user EXEC mode.

```
{passwd | password} password [encrypted]
```

```
no {passwd | password} password
```

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another FWSM but do not know the original password, you can enter the passwd command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the show running-config passwd command.
passwd password	You can enter either command; they are aliased to each other.
<i>password</i>	Sets the password as a case-sensitive string of up to 80 characters. The password must not contains spaces.

Defaults

The default password is “cisco.”

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This login password is for the default user. If you configure CLI authentication per user for Telnet or SSH using the **aaa authentication console** command, then this password is not used.

Examples

The following example sets the password to Pa\$\$w0rd:

```
hostname(config)# passwd Pa$$w0rd
```

The following example sets the password to an encrypted password that you copied from another FWSM:

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
clear configure passwd	Clears the login password.
enable	Enters privileged EXEC mode.
enable password	Sets the enable password.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config passwd	Shows the login password in encrypted form.

password (crypto ca trustpoint)

To specify a challenge phrase that is registered with the CA during enrollment, use the **password** command in crypto ca trustpoint configuration mode. The CA typically uses this phrase to authenticate a subsequent revocation request. To restore the default setting, use the **no** form of the command.

password *string*

no password

Syntax Description

string Specifies the name of the password as a character string. The first character cannot be a number. The string can contain any alphanumeric characters, including spaces, up to 80 characters. You cannot specify the password in the format number-space-anything. The space after the number causes problems. For example, hello 21 is a legal password, but 21 hello is not. The password checking is case sensitive. For example, the password Secret is different from the password secret.

Defaults

The default setting is to not include a password.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command lets you specify the revocation password for the certificate before actual certificate enrollment begins. The specified password is encrypted when the updated configuration is written to NVRAM by the FWSM.

If this command is enabled, you will not be prompted for a password during certificate enrollment.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes a challenge phrase registered with the CA in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxyyy
hostname(ca-trustpoint)#
```

Related Commands	Command	Description
	crypto ca trustpoint	Enters trustpoint configuration mode.
	default enrollment	Returns enrollment parameters to their defaults.

password-storage

To let users store their login passwords on the client system, use the **password-storage enable** command in group-policy configuration mode or username configuration mode. To disable password storage, use the **password-storage disable** command.

To remove the password-storage attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for password-storage from another group policy.

password-storage {enable | disable}

no password-storage

Syntax Description

disable	Disables password storage.
enable	Enables password storage.

Defaults

Password storage is disabled.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Enable password storage only on systems that you know to be in secure sites.

This command has no bearing on interactive hardware client authentication or individual user authentication for hardware clients.

Examples

The following example shows how to enable password storage for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

peer-id-validate

To specify whether to validate the identity of the peer using the peer certificate, use the **peer-id-validate** command in tunnel-group ipsec-attributes mode. To return to the default value, use the **no** form of this command.

peer-id-validate *option*

no peer-id-validate

Syntax Description

<i>option</i>	Specifies one of the following options:
	<ul style="list-style-type: none"> • req: required • cert: if supported by certificate • nocheck: do not check

Defaults

The default setting for this command is **req**.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Tunnel-group ipsec attributes	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-ipsec configuration mode, requires validating the peer using the identity of the peer's certificate for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# peer-id-validate req
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the configuration for the indicated tunnel group or for all tunnel groups.
tunnel-group-map default-group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

perfmon

To enable the FWSM to capture performance information on a periodic basis, use the **perfmon verbose** command in privileged EXEC mode. To disable performance information output, use the **perfmon quiet** command. To view the performance information that was captured, use the **show console-output** command.

perfmon { verbose | quiet }

Syntax Description

verbose	Captures performance information.
quiet	Disables performance monitoring.

Defaults

The default interval is 120 seconds. See the **perfmon interval** command to set the interval.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM does not include a serial console port, but some messages are only displayed on a console port, including output from the **perfmon** commands. Use the **show output-console** command to view the console buffer, including the **perfmon** command output. Alternatively, you can view the current performance information using the **show perfmon** command, which does display in a Telnet or SSH session.

Examples

This example shows how to capture the performance monitor statistics every 30 seconds:

```
hostname# perfmon interval 30
hostname# perfmon verbose
hostname# show console-output
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

Command	Description
perfmon settings	Shows the performance monitoring settings.
perfmon interval	Sets the performance monitoring capture interval.
show console-output	Shows the console buffer.
show perfmon	Displays performance information immediately.

perfmon interval

To set the interval in seconds to capture performance information, use the **perfmon interval** command in privileged EXEC mode.

perfmon interval *seconds*

Syntax Description

seconds Specifies the number of seconds before the performance display is refreshed.

Defaults

The *seconds* is 120 seconds.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

To enable performance monitoring, enter the **perfmon verbose** command. To disable it, enter the **perfmon quiet** command. The FWSM does not include a serial console port, but some messages are only displayed on a console port, including output from the **perfmon** commands. Use the **show output-console** command to view the console buffer, including the **perfmon** command output. Alternatively, you can view the current performance information using the **show perfmon** command, which does display in a Telnet or SSH session.

Examples

This example shows how to capture the performance monitor statistics every 30 seconds:

```
hostname# perfmon interval 30
hostname# perfmon verbose
```

Related Commands

Command	Description
perfmon	Enables the FWSM to capture performance monitoring information.
perfmon settings	Shows the performance monitoring settings.
show console-output	Shows the console buffer.
show perfmon	Displays performance information.

perfmon settings

To view the performance monitoring configuration settings, use the **perfmon settings** command in privileged EXEC mode.

perfmon settings

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

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

Examples This example shows how to display the **perfmon** settings:

```
hostname# perfmon settings
interval: 120 (seconds)
quiet
```

Related Commands	Command	Description
	perfmon	Enables the FWSM to capture performance monitoring information.
	perfmon interval	Sets the performance monitoring capture interval.
	show console-output	Shows the console buffer.
	show perfmon	Displays performance information immediately.

periodic

To specify a recurring (weekly) time range for functions that support the time-range feature, use the **periodic** command in time-range configuration mode. To disable, use the **no** form of this command.

periodic *days-of-the-week time to [days-of-the-week] time*

no periodic *days-of-the-week time to [days-of-the-week] time*

Syntax Description

days-of-the-week (Optional) The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect.

This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are:

- **daily**—Monday through Sunday
- **weekdays**—Monday through Friday
- **weekend**—Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, you can omit them.

time Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.

to Entry of the **to** keyword is required to complete the range “from start-time to end-time.”

Defaults

If a value is not entered with the **periodic** command, access to the FWSM as defined with the **time-range** command is in effect immediately and always on.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To implement a time-based ACL, use the **time-range** command to define specific times of the day and week. Then use the with the **access-list extended time-range** command to bind the time range to an ACL.

The **periodic** command is one way to specify when a time range is in effect. Another way is to specify an absolute time period with the **absolute** command. Use either of these commands after the **time-range** global configuration command, which specifies the name of the time range. Multiple **periodic** entries are allowed per **time-range** command.

**Note**

Overlapping time-ranges are allowed in the configuration, so if you enter one time range (8:00 to 15:00) and then enter another time range that overlaps (10:00 to 17:00), the time range is active for the union of both periodic time ranges specified (8:00 to 17:00).

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

Examples

The following examples show how to configure the **periodic** command:

If you want:	Enter this:
Monday through Friday, 8:00 a.m. to 6:00 p.m. only	periodic weekdays 8:00 to 18:00
Every day of the week, from 8:00 a.m. to 6:00 p.m. only	periodic daily 8:00 to 18:00
Every minute from Monday 8:00 a.m. to Friday 8:00 p.m.	periodic monday 8:00 to friday 20:00
All weekend, from Saturday morning through Sunday night	periodic weekend 00:00 to 23:59
Saturdays and Sundays, from noon to midnight	periodic weekend 12:00 to 23:59

The following example shows how to allow access to the FWSM on Monday through Friday, 8:00 a.m. to 6:00 p.m. only:

```
hostname(config-time-range) # periodic weekdays 8:00 to 18:00
hostname(config-time-range) #
```

The following example shows how to allow access to the FWSM on specific days (Monday, Tuesday, and Friday), 10:30 a.m. to 12:30 p.m.:

```
hostname(config-time-range) # periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range) #
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
access-list extended	Configures a policy for permitting or denying IP traffic through the FWSM.
time-range	Defines access control to the FWSM based on time.

permit

To allow invalid GTP packets or packets that otherwise would fail parsing and be dropped, or to configure trusted GSNs, use the **permit** command in GTP map configuration mode, which is accessed by using the **gtp-map** command. Use the **no** form of this command to remove the command.

```
permit {errors | {response to-object-group receive-object-group from-object-group
send-object-group}}
```

```
no {errors | {response to-object-group receive-object-group from-object-group
send-object-group}}
```

Syntax Description

errors	Allows packets with errors to be passed.
from-object-group <i>send-object-group</i>	Specifies the name of the object group sending the response.
response	Specifies an object group allowed to receive responses from another object group.
to-object-group <i>receive-object-group</i>	Specifies the name of the object group sending the requests.

Defaults

By default, all invalid packets or packets that failed, during parsing, are dropped.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.
3.2(1)	Keyword response was added.

Usage Guidelines

Use the **permit** command in GTP map configuration mode to allow invalid GTP packets or packets that otherwise would fail parsing and be dropped. You can also configure the trusted GSNs to respond to the requests of a particular GSN not specified in the GTP request.

Only object groups with IPv4 address network objects are supported. IPv6 is not supported with GTP.

Examples

The following example permits traffic containing invalid packets or packets that failed, during parsing:

```
hostname(config)# gtp-map gtp-policy
```

```
hostname(config-gtpmap)# permit errors
```

Related Commands

Commands	Description
clear service-policy inspect gtp	Clears global GTP statistics.
debug gtp	Displays detailed information about GTP inspection.
gtp-map	Defines a GTP map and enables GTP map configuration mode.
inspect gtp	Applies a specific GTP map to use for application inspection.
show service-policy inspect gtp	Displays the GTP configuration.

pfs

To enable PFS, use the **pfs enable** command in group-policy configuration mode. To disable PFS, use the **pfs disable** command. To remove the PFS attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for PFS from another group policy.

In IPSec negotiations, PFS ensures that each new cryptographic key is unrelated to any previous key.

pfs {enable | disable}

no pfs

Syntax Description

disable	Disables PFS.
enable	Enables PFS.

Defaults

PFS is disabled.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The PFS setting on the VPN client and the FWSM must match.

Examples

The following example shows how to set PFS for the group policy named FirstGroup:

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

pim

To reenable PIM on an interface, use the **pim** command in interface configuration mode. To disable PIM, use the **no** form of this command.

pim

no pim

Syntax Description

This command has no arguments or keywords.

Defaults

The **multicast-routing** command enables PIM on all interfaces by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **multicast-routing** command enables PIM on all interfaces by default. Only the **no** form of the **pim** command is saved in the configuration.



Note

PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

Examples

The following example disables PIM on the selected interface:

```
hostname(config)# interface vlan101
hostname(config-subif)# no pim
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

pim accept-register

To configure the FWSM to filter PIM register messages, use the **pim accept-register** command in global configuration mode. To remove the filtering, use the **no** form of this command.

```
pim accept-register {list acl | route-map map-name}
```

```
no pim accept-register
```

Syntax Description

list <i>acl</i>	Specifies an access list name or number. Use standard host ACLs with this command; extended ACLs are not supported.
route-map <i>map-name</i>	Specifies a route-map name. Use standard host ACLs with the route-maps referenced by this command; extended ACLs are not supported.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command is used to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the FWSM will immediately send back a register-stop message.

Examples

The following example restricts PIM register messages to those from sources defined in the access list named “no-ssm-range”:

```
hostname(config)# pim accept-register list no-ssm-range
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

pim dr-priority

To configure the neighbor priority on the FWSM used for designated router election, use the **pim dr-priority** command in interface configuration mode. To restore the default priority, use the **no** form of this command.

pim dr-priority *number*

no pim dr-priority

Syntax Description

<i>number</i>	A number from 0 to 4294967294. This number is used to determine the priority of the device when determining the designated router. Specifying 0 prevents the FWSM from becoming the designated router.
---------------	--

Defaults

The default value is 1.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The device with the largest priority value on an interface becomes the PIM designated router. If multiple devices have the same designated router priority, then the device with the highest IP address becomes the DR. If a device does not include the DR-Priority Option in hello messages, it is regarded as the highest-priority device and becomes the designated router. If multiple devices do not include this option in their hello messages, then the device with the highest IP address becomes the designated router.

Examples

The following example sets the DR priority for the interface to 5:

```
hostname(config)# interface Vlan101
hostname(config-if)# pim dr-priority 5
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

pim hello-interval

To configure the frequency of the PIM hello messages, use the **pim hello-interval** command in interface configuration mode. To restore the hello-interval to the default value, use the **no** form of this command.

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

Syntax Description

seconds The number of seconds that the FWSM waits before sending a hello message. Valid values range from 1 to 3600 seconds. The default value is 30 seconds.

Defaults

30 seconds.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example sets the PIM hello interval to 1 minute:

```
hostname(config)# interface Vlan101
hostname(config-if)# pim hello-interval 60
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

pim join-prune-interval

To configure the PIM join/prune interval, use the **pim join-prune-interval** command in interface configuration mode. To restore the interval to the default value, use the **no** form of this command.

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

Syntax Description	<i>seconds</i>	The number of seconds that the FWSM waits before sending a join/prune message. Valid values range from 10 to 600 seconds. 60 seconds is the default.
---------------------------	----------------	--

Defaults	60 seconds
-----------------	------------

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

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Examples The following example sets the PIM join/prune interval to 2 minutes:

```
hostname(config)# interface Vlan101
hostname(config-if)# pim join-prune-interval 120
```

Related Commands	Command	Description
	multicast-routing	Enables multicast routing on the FWSM.

pim old-register-checksum

To allow backward compatibility on a rendezvous point (RP) that uses old register checksum methodology, use the **pim old-register-checksum** command in global configuration mode. To generate PIM RFC-compliant registers, use the **no** form of this command.

pim old-register-checksum

no pim old-register-checksum

Syntax Description

This command has no arguments or keywords.

Defaults

The FWSM generates PIM RFC-compliant registers.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM software accepts register messages with checksum on the PIM header and only the next 4 bytes rather than using the Cisco IOS method—accepting register messages with the entire PIM message for all PIM message types. The **pim old-register-checksum** command generates registers compatible with Cisco IOS software.

Examples

The following example configures the FWSM to use the old checksum calculations:

```
hostname(config)# pim old-register-checksum
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

pim rp-address

To configure the address of a PIM rendezvous point (RP), use the **pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

```
pim rp-address ip_address [acl] [bidir]
```

```
no pim rp-address ip_address
```

Syntax Description

<i>acl</i>	(Optional) The name or number of an access list that defines which multicast groups the RP should be used with. This is a standard IP access list.
bidir	(Optional) Indicates that the specified multicast groups are to operate in bidirectional mode. If the command is configured without this option, the specified groups operate in PIM sparse mode.
<i>ip_address</i>	IP address of a router to be a PIM RP. This is a unicast IP address in four-part dotted-decimal notation.

Defaults

No PIM RP addresses are configured.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

All routers within a common PIM sparse mode (PIM-SM) or bidir domain require knowledge of the well-known PIM RP address. The address is statically configured using this command.



Note

The FWSM does not support Auto-RP; you must use the **pim rp-address** command to specify the RP address.

You can configure a single RP to serve more than one group. The group range specified in the access list determines the PIM RP group mapping. If the an access list is not specified, the RP for the group is applied to the entire IP multicast group range (224.0.0.0/4).

**Note**

The FWSM always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

Examples

The following example sets the PIM RP address to 10.0.0.1 for all multicast groups:

```
hostname(config)# pim rp-address 10.0.0.1
```

Related Commands

Command	Description
pim accept-register	Configures candidate RPs to filter PIM register messages.

pim spt-threshold infinity

To change the behavior of the last hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the **pim spt-threshold infinity** command in global configuration mode. To restore the default value, use the **no** form of this command.

```
pim spt-threshold infinity [group-list acl]
```

```
no pim spt-threshold
```

Syntax Description

group-list acl (Optional) Indicates the source groups restricted by the access list. The *acl* argument must specify a standard ACL; extended ACLs are not supported.

Defaults

The last hop PIM router switches to the shortest-path source tree by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

If the **group-list** keyword is not used, this command applies to all multicast groups.

Examples

The following example causes the last hop PIM router to always use the shared tree instead of switching to the shortest-path source tree:

```
hostname(config)# pim spt-threshold infinity
```

Related Commands

Command	Description
multicast-routing	Enables multicast routing on the FWSM.

ping

To determine if other IP addresses are visible from the FWSM, use the **ping** command in privileged EXEC mode.

ping [*if_name*] *host* [**data pattern**] [**repeat count**] [**size bytes**] [**timeout seconds**] [**validate**]

Syntax Description

data pattern	(Optional) Specifies the 16-bit data pattern in hexadecimal.
<i>host</i>	Specifies the IPv4 or IPv6 address or name of the host to ping.
<i>if_name</i>	(Optional) Specifies the interface name, as configured by the nameif command, by which the <i>host</i> is accessible. If not supplied, then the <i>host</i> is resolved to an IP address and then the routing table is consulted to determine the destination interface.
repeat count	(Optional) Specifies the number of times to repeat the ping request.
size bytes	(Optional) Specifies the datagram size in bytes.
timeout seconds	(Optional) Specifies the the number of seconds to wait before timing out the ping request.
validate	(Optional) Specifies to validate reply data.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **ping** command allows you to determine if the FWSM has connectivity or if a host is available on the network. If the FWSM has connectivity, ensure that the **icmp permit any interface** command is configured. This configuration is required to allow the FWSM to respond and accept messages generated from the **ping** command. The **ping** command output shows if the response was received. If a host is not responding, when you enter the **ping** command, a message similar to the following displays:

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

Use the **show interface** command to ensure that the FWSM is connected to the network and is passing traffic. The address of the specified *if_name* is used as the source address of the ping.

If you want internal hosts to ping external hosts, you must do one of the following:

- Create an ICMP **access-list** command for an echo reply; for example, to give ping access to all hosts, use the **access-list acl_grp permit icmp any any** command and bind the **access-list** command to the interface that you want to test using the **access-group** command.
- Configure the ICMP inspection engine using the **inspect icmp** command. For example, adding the **inspect icmp** command to the **class default_inspection** class for the global service policy allows echo replies through the FWSM for echo requests initiated by internal hosts.

You can also perform an extended ping, which allows you to enter the keywords one line at a time.

If you are pinging through the FWSM between hosts or routers, but the pings are not successful, use the **capture** command to monitor the success of the ping.

The FWSM **ping** command does not require an interface name. If you do not specify an interface name, the FWSM checks the routing table to find the address that you specify. You can specify an interface name to indicate through which interface the ICMP echo requests are sent.

Examples

The following example shows how to determine if other IP addresses are visible from the FWSM:

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The following is an example of an extended ping:

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

Related Commands

Command	Description
capture	Captures packets at an interface
icmp	Configures access rules for ICMP traffic that terminates at an interface.
show interface	Displays information about the VLAN configuration.

policy

To specify the source for retrieving the CRL, use the **policy** command in `crl configure` configuration mode. `crl configure` configuration mode is accessible from `crypto ca trustpoint` configuration mode. To restore the default setting, use the **no** form of the command.

policy {static | cdp | both}

no policy [static | cdp | both]

Syntax Description

both	Specifies that if obtaining a CRL using the CRL distribution point fails, retry using static CDPs up to a limit of five.
cdp	Uses the CDP extension embedded within the certificate being checked. In this case, the FWSM retrieves up to five CRL distribution points from the CDP extension of the certificate being verified and augments their information with the configured default values, if necessary. If the FWSM attempt to retrieve a CRL using the primary CDP fails, it retries using the next available CDP in the list. This continues until either the FWSM retrieves a CRL or exhausts the list.
static	Uses up to five static CRL distribution points. If you specify this option, specify also the LDAP or HTTP URLs with the protocol command.

Defaults

The default setting is **cdp**.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters `ca-crl` configuration mode, and configures CRL retrieval to occur using the CRL distribution point extension in the certificate being checked or if that fails, to use static CDPs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
url	Creates and maintains a list of static URLs for retrieving CRLs.

policy-map

To configure a policy, use the **policy-map** command in global configuration mode. To remove a policy, use the **no** form of this command.

policy-map *name*

no policy-map *name*

Syntax Description

name The name for this policy-map. The name can be up to 40 characters long.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

A **policy-map** command configures a policy, which is an association of a traffic class with one or more security-related actions. A traffic class is a set of traffic that is identifiable by its packet content. For example, TCP traffic with a port value of 23 can be classified as a Telnet traffic class. A policy consists of a **class** command and its associated actions. A policy map can specify multiple policies. A **service-policy** command activates a policy map globally on all interfaces or on a single targeted interface.

The **policy-map** command lets you classify traffic and then apply feature-specific actions to it.

The maximum number of policy maps is 64.

Use the **policy-map** command to enter policy-map mode, in which you can enter **class** and **description** commands. See the individual command descriptions for detailed information.

The order in which different types of actions in a policy-map are performed is independent of the order in which the actions appear in these command descriptions.

Examples

The following is an example of the **policy-map** command; note the change in the prompt:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)#
```

The following is an example of a **policy-map** command for connection policy:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server

hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit

hostname(config)# policy-map global-policy global
hostname(config-pmap)# description This policy map defines a policy concerning connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

Related Commands

Command	Description
class	Specifies a class-map for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
description	Specifies a description for the policy-map.
show running-config policy-map	Display all current policy-map configurations.

polltime interface

To specify the interval between hello packets on the interface, use the **polltime interface** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

polltime interface *time*

no polltime interface *time*

Syntax Description

time Amount of time between hello messages.

Defaults

The default is 15 seconds.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **polltime interface** command to change the frequency that hello packets are sent out on an interfaces associated with the current failover group. With a faster poll time, the FWSM can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested.

Five missed consecutive interface hello packets cause interface testing.

This command is available for Active/Active failover only.

Examples

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

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface 20
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover polltime	Configures the time between hello packets on monitored interfaces.

port-misuse

To restrict HTTP traffic by specifying a restricted application category, use the **port-misuse** command in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

```
port-misuse {im | p2p | tunneling | default} action {allow | reset | drop} [log]
```

```
no port-misuse {im | p2p | tunneling | default} action {allow | reset | drop} [log]
```

Syntax Description

action	Specifies the action taken when an application in the configured category is detected.
allow	Allows the message.
default	Specifies the default action taken by the FWSM when the traffic contains a supported request method that is not on a configured list.
im	Restricts traffic in the instant messaging application category. The applications checked for are Yahoo Messenger, AIM, and MSN IM.
log	(Optional) Generates a syslog.
p2p	Restricts traffic in the peer-to-peer application category. The Kazaa application is checked.
reset	Sends a TCP reset message to client and server.
tunneling	Restricts traffic in the tunneling application category. The applications checked for are: HTTPPort/HTTHost, GNU Httptunnel, GotoMyPC, Firethru, and Http-tunnel.com Client.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enable the **port-misuse** command, the FWSM applies the specified action to HTTP connections for each supported and configured application category.

The FWSM applies the **default** action to all traffic that does *not* match the application categories on the configured list. The preconfigured **default** action is to **allow** connections without logging.

For example, given the preconfigured default action, if you specify one or more application categories with the action of **drop** and **log**, the FWSM drops connections containing the configured application categories, logs each connection, and allows all connections for the other supported application types.

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

Enter the **port-misuse** command once for each setting you wish to apply. You use one instance of the **port-misuse** command to change the default action and one instance to add each application category to the list of configured application types.



Caution

These inspections require searches in the entity body of the HTTP message and may affect the performance of the FWSM.

When you use the **no** form of the command to remove an application category from the list of configured application types, any characters in the command line after the application category keyword are ignored.

Examples

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

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse p2p drop log
hostname(config-http-map)# exit
```

In this case, only connections in the peer-to-peer category are dropped and the events is logged.

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

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse im allow
hostname(config-http-map)# exit
```

In this case, only the Instant Messenger application is allowed. When HTTP traffic for the other supported applications is received, the FWSM resets the connection and creates a syslog entry.

Related Commands

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

port-object

To add a port object to a service object group, use the **port-object** command in service configuration mode. To remove port objects, use the **no** form of this command.

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

Syntax Description

begin_service	Specifies the decimal number or name of a TCP or UDP port that is the beginning value for a range of services. This value must be between 0 and 65535.
end_service	Specifies the decimal number or name of a TCP or UDP port that is the ending value for a range of services. This value must be between 0 and 65535.
eq service	Specifies the decimal number or name of a TCP or UDP port for a service object.
range	Specifies a range of ports (inclusive).

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **port-object** command is used with the **object-group** command to define an object that is either a specific service (port) or a range of services (ports) in service configuration mode.

If a name is specified for a TCP or UDP service, it must be one of the supported TCP or/and UDP names, and must be consistent with the protocol type of the object group. For instance, for a protocol types of tcp, udp, and tcp-udp, the names must be a valid TCP service name, a valid UDP service name, or a valid TCP and UDP service name, respectively.

If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object.

The following service names are supported:

Table 22-1

TCP	UDP	TCP and UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

Examples

The following example shows how to use the **port-object** command in service configuration mode to create a new port (service) object group:

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
```

```

hostname(config-service)# port-object eq snmp
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit

```

Related Commands

Command	Description
clear configure object-group	Removes all the object-group commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

preempt

To cause the unit to become active on boot if it has the higher priority, use the **preempt** command in failover group configuration mode. To remove the preemption, use the **no** form of this command.

preempt [*delay*]

no preempt [*delay*]

Syntax Description

delay The wait time, in seconds, before the peer is preempted. Valid values are from 1 to 1200 seconds.

Defaults

By default, there is no delay.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). However, if one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command. If the failover group is configured with the **preempt** command, the failover group automatically becomes active on the designated unit.



Note

If Stateful Failover is enabled, the preemption is delayed until the connections are replicated from the unit on which the failover group is currently active.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command with a wait time of 100 seconds, so the groups will automatically become active on their preferred unit 100 seconds after the units become available.

```
hostname(config)# failover group 1
```

```

hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#

```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
primary	Gives the primary unit in a failover pair priority for the failover group being configured.
secondary	Gives the secondary unit in a failover pair priority for the failover group being configured.

prefix-list

To create an entry in a prefix list for ABR type 3 LSA filtering, use the **prefix-list** command in global configuration mode. To remove a prefix list entry, use the **no** form of this command.

```
prefix-list prefix-list-name [seq seq_num] {permit | deny} network/len [ge min_value] [le max_value]
```

```
no prefix-list prefix-list-name [seq seq_num] {permit | deny} network/len [ge min_value] [le max_value]
```

Syntax Description

<i>/</i>	A required separator between the <i>network</i> and <i>len</i> values.
deny	Denies access for a matching condition.
ge <i>min_value</i>	(Optional) Specifies the minimum prefix length to be matched. The value of the <i>min_value</i> argument must be greater than the value of the <i>len</i> argument and less than or equal to the <i>max_value</i> argument, if present.
le <i>max_value</i>	(Optional) Specifies the maximum prefix length to be matched. The value of the <i>max_value</i> argument must be greater than or equal to the value of the <i>min_value</i> argument, if present, or greater than the value of the <i>len</i> argument if the <i>min_value</i> argument is not present.
<i>len</i>	The length of the network mask. Valid values are from 0 to 32.
<i>network</i>	The network address.
permit	Permits access for a matching condition.
<i>prefix-list-name</i>	The name of the prefix list. The prefix-list name cannot contain spaces.
seq <i>seq_num</i>	(Optional) Applies the specified sequence number to the prefix list being created.

Defaults

If you do not specify a sequence number, the first entry in a prefix list is assigned a sequence number of 5, and the sequence number for each subsequent entry is increased by 5.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced (as ip prefix-list).
3.1(1)	This command was changed from ip prefix-list to prefix-list .

Usage Guidelines

The **prefix-list** commands are ABR type 3 LSA filtering commands. ABR type 3 LSA filtering extends the capability of an ABR that is running OSPF to filter type 3 LSAs between different OSPF areas. Once a prefix list is configured, only the specified prefixes are sent from one area to another area. All other prefixes are restricted to their OSPF area. You can apply this type of area filtering to traffic going into or coming out of an OSPF area, or to both the incoming and outgoing traffic for that area.

When multiple entries of a prefix list match a given prefix, the entry with the lowest sequence number is used. The FWSM begins the search at the top of the prefix list, with the entry with the lowest sequence number. Once a match is made, the FWSM does not go through the rest of the list. For efficiency, you may want to put the most common matches or denials near the top of the list by manually assigning them a lower sequence number.

By default, the sequence numbers are automatically generated. They can be suppressed with the **no prefix-list sequence-number** command. Sequence numbers are generated in increments of 5. The first sequence number generated in a prefix list would be 5. The next entry in that list would have a sequence number of 10, and so on. If you specify a value for an entry, and then do not specify values for subsequent entries, the generated sequence numbers are increased from the specified value in increments of 5. For example, if you specify that the first entry in the prefix list has a sequence number of 3, and then add two more entries without specifying a sequence number for the additional entries, the automatically generated sequence numbers for those two entries would be 8 and 13.

You can use the **ge** and **le** keywords to specify the range of the prefix length to be matched for prefixes that are more specific than the *network/len* argument. Exact match is assumed when neither the **ge** or **le** keywords are specified. The range is from *min_value* to 32 if only the **ge** keyword is specified. The range is from *len* to *max_value* if only the **le** keyword is specified.

The value of the *min_value* and *max_value* arguments must satisfy the following condition:

$$len < min_value \leq max_value \leq 32$$

Use the **no** form of the command to remove specific entries from the prefix list. Use the **clear configure prefix-list** command to remove a prefix list. The clear **configure prefix-list** command also removes the associated **prefix-list description** command, if any, from the configuration.

Examples

The following example denies the default route 0.0.0.0/0:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

The following example permits the prefix 10.0.0.0/8:

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

The following example shows how to accept a mask length of up to 24 bits in routes with the prefix 192/8:

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in routes with a prefix of 192/8:

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

The following example shows how to permit mask lengths from 8 to 24 bits in all address space:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

The following example shows how to deny mask lengths greater than 25 bits in all address space:

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

The following example shows how to deny all routes with a prefix of 10/8:

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

The following example shows how to deny all masks with a length greater than 25 bits for routes with a prefix of 192.168.1/24:

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

The following example shows how to permit all routes with a prefix of 0/0:

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

Related Commands

Command	Description
clear configure prefix-list	Removes the prefix-list commands from the running configuration.
prefix-list description	Lets you to enter a description for a prefix list.
prefix-list sequence-number	Enables prefix list sequence numbering.
show running-config prefix-list	Displays the prefix-list commands in the running configuration.

prefix-list description

To add a description to a prefix list, use the **prefix-list description** command in global configuration mode. To remove a prefix list description, use the **no** form of this command.

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

Syntax Description

<i>prefix-list-name</i>	The name of a prefix list.
<i>text</i>	The text of the prefix list description. You can enter a maximum of 80 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can enter **prefix-list** and **prefix-list description** commands in any order for a particular prefix list name; you do not need to create the prefix list before entering a prefix list description. The **prefix-list description** command will always appear on the line before the associated prefix list in the configuration, no matter what order you enter the commands.

If you enter a **prefix-list description** command for a prefix list entry that already has a description, the new description replaces the original description.

You do not need to enter the text description when using the **no** form of this command.

Examples

The following example adds a description for a prefix list named MyPrefixList. The **show running-config prefix-list** command shows that although the prefix list description has been added to the running configuration, the prefix-list itself has not been configured.

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list description
hostname(config)# show running-config prefix-list
```

```
!
prefix-list MyPrefixList description A sample prefix list description
```

!

Related Commands

Command	Description
clear configure prefix-list	Removes the prefix-list commands from the running configuration.
prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
show running-config prefix-list	Displays the prefix-list commands in the running configuration.

prefix-list sequence-number

To enable prefix list sequence numbering, use the **prefix-list sequence-number** command in global configuration mode. To disable prefix list sequence numbering, use the **no** form of this command.

prefix-list sequence-number

Syntax Description This command has no arguments or keywords.

Defaults Prefix list sequence numbering is enabled by default.

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

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines Only the **no** form of this command appears in the configuration. When the **no** form of this command is in the configuration, the sequence numbers, including the manually configured ones, are removed from the **prefix-list** commands in the configuration and new prefix lists entries are not assigned a sequence number.

When prefix list sequence numbering is enabled, all prefix list entries are assigned sequence numbers using the default numbering method (starting with 5 and incrementing each number by 5). If a sequence number was manually assigned to a prefix list entry before numbering was disabled, the manually assigned number is restored. Sequence numbers that are manually assigned while automatic numbering is disabled are also restored, even though they are not displayed while numbering is disabled.

Examples The following example disables prefix list sequence numbering:

```
hostname(config)# no prefix-list sequence-number
```

Related Commands	Command	Description
	prefix-list	Defines a prefix list for ABR type 3 LSA filtering.
	show running-config prefix-list	Displays the prefix-list commands in the running configuration.

pre-shared-key

To specify a preshared key to support IKE connections based on preshared keys, use the **pre-shared-key** command in tunnel-group ipsec-attributes configuration mode. To return to the default value, use the **no** form of this command.

pre-shared-key *key*

no pre-shared-key

Syntax Description

key Specifies an alphanumeric key between 1 and 128 characters.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute to all tunnel-group types.

Examples

The following command entered in config-ipsec configuration mode, specifies the preshared key XYZX to support IKE connections for the IPsec LAN-to-LAN tunnel group named 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPsec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config-ipsec)#
```

Related Commands

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

primary

To give the primary unit higher priority for a failover group, use the **primary** command in failover group configuration mode. To restore the default value, use the **no** form of this command.

primary

no primary

Syntax Description

This command has no arguments or keywords.

Defaults

If **primary** or **secondary** is not specified for a failover group, the failover group defaults to **primary**.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Assigning a primary or secondary priority to a failover group specifies which unit the failover group becomes active on when both units boot simultaneously (within a unit polltime). If one unit boots before the other, then both failover groups become active on that unit. When the other unit comes online, any failover groups that have the second unit as a priority do not become active on the second unit unless the failover group is configured with the **preempt** command or is manually forced to the other unit with the **no failover active** command.

Examples

The following example configures failover group 1 with the primary unit as the higher priority and failover group 2 with the secondary unit as the higher priority. Both failover groups are configured with the **preempt** command, so the groups will automatically become active on their preferred unit as the units become available.

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands	Command	Description
	failover group	Defines a failover group for Active/Active failover.
	preempt	Forces the failover group to become active on its preferred unit when the unit becomes available.
	secondary	Gives the secondary unit a higher priority than the primary unit.

privilege

To configure the command privilege levels, use the **privilege** command in global configuration mode. To disallow the configuration, use the **no** form of this command.

privilege [**show** | **clear** | **configure**] **level** *level* [**mode** { **enable** | **configure** }] **command** *command*

no privilege [**show** | **clear** | **configure**] **level** *level* [**mode** { **enable** | **configure** }] **command** *command*

Syntax Description

clear	(Optional) Sets the privilege level for the clear command corresponding to the command specified.
command <i>command</i>	Specifies the command on which to set the privilege level.
configure	(Optional) Sets the privilege level for the command specified.
level <i>level</i>	Specifies the privilege level; valid values are from 0 to 15.
mode enable	(Optional) Indicates that the level is for the enable mode of the command.
mode configure	(Optional) Indicates that the level is for the configure mode of the command.
show	(Optional) Sets the privilege level for the show command corresponding to the command specified.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **privilege** command lets you set user-defined privilege levels for the FWSM commands. In particular, this command is useful for setting different privilege levels for related configuration, show, and clear commands. Make sure that you verify privilege level changes in your commands with your security policies before using the new privilege levels.

When commands and users have privilege levels set, the two are compared to determine if a given user can execute a given command. If the user's privilege level is lower than the privilege level of the command, the user is prevented from executing the command.

To change between privilege levels, use the **login** command to access another privilege level and the appropriate **logout**, **exit**, or **quit** command to exit that level.

The **mode enable** and **mode configure** keywords are for commands with both enable and configure modes.

Lower privilege level numbers are lower privilege levels.

**Note**

The **aaa authentication** and **aaa authorization** commands need to include any new privilege levels that you define before you can use them in your AAA server configuration.

Examples

This example shows how to set the privilege level “5” for an individual user as follows:

```
hostname(config)# username intern1 password pass1 privilege 5
```

This example shows how to define a set of **show** commands with the privilege level “5” as follows:

```
hostname(config)# privilege show level 5 command alias
hostname(config)# privilege show level 5 command apply
hostname(config)# privilege show level 5 command arp
hostname(config)# privilege show level 5 command auth-prompt
hostname(config)# privilege show level 5 command blocks
```

This example shows how to apply privilege level 11 to a complete AAA authorization configuration:

```
hostname(config)# privilege configure level 11 command aaa
hostname(config)# privilege configure level 11 command aaa-server
hostname(config)# privilege configure level 11 command access-group
hostname(config)# privilege configure level 11 command access-list
hostname(config)# privilege configure level 11 command activation-key
hostname(config)# privilege configure level 11 command age
hostname(config)# privilege configure level 11 command alias
hostname(config)# privilege configure level 11 command apply
```

Related Commands

Command	Description
clear configure privilege	Remove privilege command statements from the configuration.
show curpriv	Display current privilege level.
show running-config privilege	Display privilege levels for commands.

prompt

To customize the CLI prompt, use the **prompt** command in global configuration mode. To revert to the default prompt, use the **no** form of this command.

```
prompt {[hostname] [context] [domain] [slot] [state] [priority]}
```

```
no prompt [hostname] [context] [domain] [slot] [state] [priority]
```

Syntax Description

context	(Multiple mode only) Displays the current context.
domain	Displays the domain name.
hostname	Displays the hostname.
priority	Displays the failover priority as pri (primary) or sec (secondary). Set the priority using the failover lan unit command.
slot	Displays the slot location in the switch.
state	Displays the traffic-passing state of the unit. The following values are displayed for the state keyword: <ul style="list-style-type: none"> act—Failover is enabled, and the unit is actively passing traffic. stby— Failover is enabled, and the unit is not passing traffic and is in a standby, failed, or other non-active state. actNoFailover—Failover is not enabled, and the unit is actively passing traffic. stbyNoFailover—Failover is not enabled, and the unit is not passing traffic. This might happen when there is an interface failure above the threshold on the standby unit.

Defaults

The default prompt is the hostname. In multiple context mode, the hostname is followed by the current context name (*hostname/context*).

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The order in which you enter the keywords determines the order of the elements in the prompt, which are separated by a slash (/).

In multiple context mode, you can view the extended prompt when you log in to the system execution space or the admin context. Within a non-admin context, you only see the default prompt, which is the hostname and the context name.

The ability to add information to a prompt allows you to see at-a-glance which module you are logged into when you have multiple modules. During a failover, this feature is useful when both modules have the same hostname.

Examples

The following example shows all available elements in the prompt:

```
hostname(config)# prompt hostname context priority slot state
```

The prompt changes to the following string:

```
hostname/admin/pri/6/act(config)#
```

Related Commands

Command	Description
clear configure prompt	Clears the configured prompt.
show running-config prompt	Displays the configured prompt.

protocol http

To specify HTTP as a permitted distribution point protocol for retrieving a CRL, use the **protocol http** command in **crl configure** configuration mode. **Crl configure** configuration mode is accessible from **crypto ca trustpoint** configuration mode. To remove HTTP as the permitted method of CRL retrieval, use the **no** form of this command. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

protocol http

no protocol http

Syntax Description This command has no arguments or keywords.

Defaults The default setting is to permit HTTP.

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

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines If you use this command, be sure to assign HTTP rules to the public interface filter.

Examples The following example enters **crl configure** configuration mode, and permits HTTP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
hostname(ca-crl)#
```

Related Commands	Command	Description
	crl configure	Enters ca-crl configuration mode.
	crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
protocol ldap	Specifies LDAP as a retrieval method for CRLs.
protocol scep	Specifies SCEP as a retrieval method for CRLs.

protocol ldap

To specify LDAP as a distribution point protocol for retrieving a CRL, use the **protocol ldap** command in `crl configure` configuration mode. `Crl configure` configuration mode is accessible from `crypto ca trustpoint` configuration mode. To remove the LDAP protocol as the permitted method of CRL retrieval, use the **no** form of this command. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

protocol ldap

no protocol ldap

Syntax Description This command has no arguments or keywords.

Defaults The default setting is to permit LDAP.

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

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

Command History	Release	Modification
	3.1(1)	This command was introduced.

Examples The following example enters `crl configure` configuration mode, and permits LDAP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
hostname(ca-crl)#
```

Related Commands	Command	Description
	crl configure	Enters <code>ca-crl</code> configuration mode.
	crypto ca trustpoint	Enters trustpoint configuration mode.
	protocol http	Specifies HTTP as a retrieval method for CRLs
	protocol scep	Specifies SCEP as a retrieval method for CRLs

protocol scep

To specify SCEP as a distribution point protocol for retrieving a CRL, use the **protocol scep** command in `crl configure` configuration mode. `Crl configure` configuration mode is accessible from `crypto ca trustpoint` configuration mode. To remove the SCEP protocol as the permitted method of CRL retrieval, use the **no** form of this command. Subject to permission, the content of the CRL distribution point determines the retrieval method (HTTP, LDAP, and/or SCEP).

protocol scep

no protocol scep

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to permit SCEP.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters `crl configure` configuration mode, and permits SCEP as a distribution point protocol for retrieving a CRL for trustpoint central:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters <code>ca-crl</code> configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
protocol http	Specifies HTTP as a retrieval method for CRLs
protocol ldap	Specifies LDAP as a retrieval method for CRLs

protocol-object

To add a protocol object to a protocol object group, use the **protocol-object** command in protocol configuration mode. To remove port objects, use the **no** form of this command.

protocol-object *protocol*

no protocol-object *protocol*

Syntax Description

protocol Protocol name or number.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **protocol-object** command is used with the **object-group** command to define a protocol object in protocol configuration mode.

You can specify an IP protocol name or number using the *protocol* argument. The udp protocol number is 17, the tcp protocol number is 6, and the egp protocol number is 47.

Examples

The following example shows how to define protocol objects:

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
object-group	Defines object groups to optimize your configuration.
show running-config object-group	Displays the current object groups.

pwd

To display the current working directory, use the **pwd** command in privileged EXEC mode.

pwd

Syntax Description This command has no arguments or keywords.

Defaults The root directory (/) is the default.

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

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

Command History	Release	Modification
	3.1(1)	Support for this command was introduced.

Usage Guidelines This command is similar in functionality to the **dir** command.

Examples The following example shows how to display the current working directory:

```
hostname# pwd
flash:
```

Related Commands	Command	Description
	cd	Changes the current working directory to the one specified.
	dir	Displays the directory contents.
	more	Displays the contents of a file.

