CHAPTER 31

shun through sysopt uauth allow-http-cache Commands

shun

To block connections from an attacking host, use the **shun** command in privileged EXEC mode. To disable a shun, use the **no** form of this command.

shun *source_ip* [*dest_ip source_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *source_ip* [**vlan** *vlan_id*]

Syntax Description

dest_port	(Optional) Specifies the destination port of a current connection that you want to drop when you place the shun on the source IP address.
dest_ip	(Optional) Specifies the destination address of a current connection that you want to drop when you place the shun on the source IP address.
protocol	(Optional) Specifies the IP protocol of a current connection that you want to drop when you place the shun on the source IP address, such as UDP or TCP. By default, the protocol is 0 (any protocol).
source_ip	Specifies the address of the attacking host. If you only specify the source IP address, all future connections from this address are dropped; current connections remain in place. To drop a current connection and also place the shun, specify the additional parameters of the connection. Note that the shun remains in place for all future connections from the source IP address, regardless of destination parameters.
source_port	(Optional) Specifies the source port of a current connection that you want to drop when you place the shun on the source IP address.
vlan_id	(Optional) Specifies the VLAN ID where the source host resides.

Defaults

The default protocol is 0 (any protocol).

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **shun** command lets you block connections from an attacking host. All future connections from the source IP address are dropped and logged until the blocking function is removed manually or by the Cisco IPS sensor. The blocking function of the **shun** command is applied whether or not a connection with the specified host address is currently active.

If you specify the destination address, source and destination ports, and the protocol, then you drop the matching connection as well as placing a shun on all future connections from the source IP address; all future connections are shunned, not just those that match these specific connection parameters.

You can only have one **shun** command per source IP address.

Because the **shun** command is used to block attacks dynamically, it is not displayed in the FWSM configuration.

Whenever an interface configuration is removed, all shuns that are attached to that interface are also removed. If you add a new interface or replace the same interface (using the same name), then you must add that interface to the IPS sensor if you want the IPS sensor to monitor that interface.

Examples

The following 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
```

Apply the **shun** command using the following options:

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

The command deletes the specific current connection from the FWSM connection table and also prevents all future packets from 10.1.1.27 from going through the FWSM.

Related Commands

Command	Description
clear shun	Disables all the shuns that are currently enabled and clears the shun statistics.
show conn	Shows all active connections.
show shun	Displays the shun information.

shutdown

To disable an interface, use the **shutdown** command in interface configuration mode. To enable an interface, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

All physical interfaces are shut down by default. Allocated interfaces in security contexts are not shut down in the configuration.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

Examples

The following example enables a subinterface:

```
hostname(config)# interface gigabitethernet2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example shuts down the subinterface:

```
hostname(config)# interface gigabitethernet2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

Related Commands

Command	Description
clear xlate	Resets all translations for existing connections, causing the connections to be reset.
interface	Configures an interface and enters interface configuration mode.

sip-map

To identify a SIP application inspection map, which is required to enable the IP Address Privacy feature, use the **sip-map** command in global configuration mode. To remove the map, use the **no** form of this command.

sip-map *map_name*

no sip-map *map_name*

Syntax Description

map_name	The name of the SIP map.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
FWSM 3.1	This command was introduced.

Usage Guidelines

Use the **sip-map** command to identify a SIP application inspection map, which is required to enable the IP Address Privacy feature. When you enter this command, the system enters the SIP map configuration mode, which lets you enter the **ip-address-privacy** command. After defining the SIP map, you use the **inspect sip** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify SIP traffic, define a SIP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list sip-acl permit tcp any any eq 5060
hostname(config)# class-map sip-port
hostname(config-cmap)# match access-list sip-acl
hostname(config-cmap)# sip-map inbound_sip
hostname(config-sip-map)# ip-address-privacy
hostname(config-sip-map)# policy-map S1_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip s1_policy
hostname(config)#
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
ip-address-privacy	Enables the IP Address Privacy feature for SIP application inspection.
inspect sip	Enables SIP application inspection.
policy-map	Associates a class map with specific security actions.

size

To change the size of a memory partition, use the **size** command in resource partition configuration mode. To restore the size to the default value, use the **no** form of this command.

size *number_of_rules*

no size *number_of_rules*

Syntax Description

number_of_rules	Specifies the number of rules you want to assign to the partition.

Defaults

The default size of a partition depends on the total number of partitions. To view the default partition sizes, enter the **show resource partition** command.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The FWSM lets you set the memory size of each partition.

Important Guidelines

Caution Failure to follow these guidelines might result in dropped access list configuration as well as other anomalies, including ACL tree corruption.

- The target partition and rule allocation settings must be carefully calculated, planned, and preferably tested in a non-production environment prior to making the change to ensure that all existing contexts and rules can be accommodated.
- When failover is used, both FWSMs need to be reloaded at the same time after making partition changes. Reloading both FWSMs causes an outage with no possibility for a zero-downtime reload. At no time should two FWSMs with a mismatched number of partitions or rule limits synchronize over failover.
- Changing the partition sizes requires you to reload the FWSM.

- Change the number of partitions before you set the partition sizes using the **resource acl-partition** command; changing the number of partitions affects the overall number of rules per partition. If you increase the number of partitions, for example, then the number of rules available per partition will be smaller. Therefore, your partition size configuration might be invalid, and you might need to reconfigure all your partition sizes. Changing the number of partitions requires you to reload the FWSM before you change the partition sizes; then changing the partition sizes requires a second reload.
- Allocate contexts to specific partitions before you set the partition sizes (see the **allocate-acl-partition** command). If you plan all your partition sizes based on the contexts currently assigned to a partition, but you did not specifically allocate the contexts, then you run the risk of context assignments shifting after a reload (for example if you add or subtract contexts).
- Reduce the size of partition(s) before increasing the size of other partition(s).
- If the existing number of ACEs does not fit into the new partition size, then the resizing is rejected.
- In addition to the memory partitions to which the FWSM assigns contexts, the FWSM uses a backup tree partition to process changes to rules so traffic can continue to use the old configuration until the new configuration is ready. The backup tree must be as large as the largest partition. Therefore, some memory is automatically assigned to the backup tree in tandem with the largest partition; so be sure to include the backup tree in your calculations.
- If you reduce the size of a partition, the FWSM checks the rule allocation (see the **resource rule** or **rule** command). If you manually allocated rules between features so that the total number of rules allocated is now greater than those available, then the FWSM rejects the resizing of the partition. Similarly, if the absolute maximum number of rules for a feature is now exceeded, then the FWSM rejects the resizing of the partition.

Examples

To view the rules available for increasing partition sizes, enter the **show resource partition** command.

For example, if you reduced the sizes of partitions 0 through 5 to 15,000, then the output shows that you have 25,314 rules to reallocate to other partitions.

```
hostname(config)# show resource partition

                          Bootup     Current
 Partition    Default  Partition   Configured
  Number       Size       Size        Size
-----------+---------+----------+-----------
      0       19219      19219       15000
      1       19219      19219       15000
      2       19219      19219       15000
      3       19219      19219       15000
      4       19219      19219       15000
      5       19219      19219       15000
      6       19219      19219       19219
      7       19219      19219       19219
      8       19219      19219       19219
      9       19219      19219       19219
     10       19219      19219       19219
     11       19219      19219       19219
backup tree   19219      19219       19219
-----------+---------+----------+-----------
   Total      249847     249847      224533

Total Partition size - Configured size = Available to allocate
        249847       -     224533 =              25314
```

If you want to distribute the rules evenly across the other 6 partitions plus the backup tree, then you can add 3616 rules to each (with 2 left over). Remember that the backup tree must be as large as the largest partition, so you must consider the backup tree in your calculations. For example, if you want to make partition 6 have 24,001 rules, then you can allocate the rules like this:

Partition	Bootup Partition Size	Configured Size	Difference
6	19219	24001	4782
Backup Tree	19219	24001	4782
7	19219	22369	3150
8	19219	22369	3150
9	19219	22369	3150
10	19219	22369	3150
11	19219	22369	3150
			Total: 25314

You can also view the current mapping of contexts to partitions using the **show resource acl-partition** command.

Examples

The following example reduces partitions 0 and 1 to 40000, while increasing partitions 2 and 3 to 56616 and 56615 respectively.

```
hostname(config)# show resource partition

                        Bootup     Current
 Partition   Default  Partition   Configured
  Number       Size      Size         Size
-----------+---------+----------+-----------
      0       49970      49970       49970
      1       49969      49969       49969
      2       49969      49969       49969
      3       49969      49969       49969
backup tree   49970      49970       49970
-----------+---------+----------+-----------
   Total      249847     249847      249847

Total Partition size - Configured size = Available to allocate
              249847 -          249847 =          0

hostname(config)# resource partition 0
hostname(config-partition)# size 40000
hostname(config-partition)# resource partition 1
hostname(config-partition)# size 40000

hostname(config-partition)# show resource partition

                        Bootup     Current
 Partition   Default  Partition   Configured
  Number       Size      Size         Size
-----------+---------+----------+-----------
      0       49970      49970       40000
      1       49969      49969       40000
      2       49969      49969       49969
      3       49969      49969       49969
```

```
backup tree   49970      49970       49969
-----------+---------+----------+-----------
   Total     249847     249847      249847

Total Partition size - Configured size = Available to allocate
              249847 -          229907 =          19940

hostname(config-partition)# resource partition 2
hostname(config-partition)# size 56616
hostname(config-partition)# resource partition 3
hostname(config-partition)# size 56615

hostname(config-partition)# show resource partition

                        Bootup     Current
 Partition   Default  Partition   Configured
  Number       Size      Size        Size
-----------+---------+----------+-----------
      0       49970      49970       40000
      1       49969      49969       40000
      2       49969      49969       56616
      3       49969      49969       56615
backup tree   49970      49970       56616
-----------+---------+----------+-----------
   Total     249847     249847      249847

Total Partition size - Configured size = Available to allocate
              249847 -          249847 =          0

hostname(config-partition)# reload
```

Related Commands

Command	Description
allocate-acl-partition	Assigns a context to a specific memory partition.
clear configure resource partition	Clears the current memory partition configuration.
resource acl-partition	Sets the total number of memory partitions.
resource partition	Customizes a memory partition.
resource rule	Reallocates rules between features globally for all partitions.
rule	Reallocates rules between features for a specific partition.
show resource acl-partition	Shows the current memory partition characteristics, including the sizes and allocated contexts.
show resource partition	Shows the memory partition sizes.
show resource rule	Shows the current allocation of rules.
show running-config resource partition	Shows the current memory partition configuration.

smtp-server

To configure an SMTP server, use the **smtp-server** command in global configuration mode. To remove the attribute from the configuration, use the **no** version of this command.

The FWSM includes an internal SMTP client that the Events system can use to notify external entities that a certain event has occurred. You can configure SMTP servers to receive these event notices, and then forward them to specified e-mail addresses. The SMTP facility is active only when you enable E-mail events an the FWSM.

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

Syntax Description

primary_server	Identifies the primary SMTP server. Use either an IP address or DNS name
backup_server	Identifies a backup SMTP server to relay event messages in the event the primary SMTP server is unavailable. Use either an IP address or DNS name.

Defaults

No SMTP server is configured by default.

Command Modes

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

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

Command History

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

Usage Guidelines

Examples

The following example shows how to set an SMTP server with an IP address of 10.1.1.24, and a backup SMTP server with an IP address of 10.1.1.34:

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

snmp-map

To identify a specific map for defining the parameters for SNMP inspection, use the **snmp-map** command in global configuration mode. To remove the map, use the **no** form of this command.

snmp-map *map_name*

no snmp-map *map_name*

Syntax Description

map_name	The name of the SNMP map.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **snmp-map** command to identify a specific map to use for defining the parameters for SNMP inspection. When you enter this command, the system enters the SNMP map configuration mode, which lets you enter the different commands used for defining the specific map. After defining the SNMP map, you use the **inspect snmp** command to enable the map. Then you use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface.

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
deny version	Disallows traffic using a specific version of SNMP.
inspect snmp	Enable SNMP application inspection.
policy-map	Associates a class map with specific security actions.

snmp-server community

To set the SNMP community string, use the **snmp-server community** command in global configuration mode. To remove the community string, use the **no** form of this command.

snmp-server community *text*

no snmp-server community [*text*]

Syntax Description

text	Sets the community string.

Defaults

By default, the community string is **public**.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

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.

Note If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example sets the community string to wallawallabingbang:

```
hostname(config)# snmp-server community wallawallabingbang
```

Related Commands

Command	Description
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the FWSM.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server contact

To set the SNMP contact name, use the **snmp-server contact** command in global configuration mode. To remove the contact name, use the **no** form of this command.

snmp-server contact *text*

no snmp-server contact [*text*]

Syntax Description

text	Specifies the name of the contact person or the FWSM system administrator. The name is case sensitive and can be up to 127 characters. Spaces are accepted, but multiple spaces are shortened to a single space.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example sets the contact as Pat Johnson:

```
hostname(config)# snmp-server contact Pat Johnson
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server enable	Enables SNMP on the FWSM.
snmp-server enable traps	Enables SNMP traps.

Command	Description
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable

To enable the SNMP server on the FWSM, use the **snmp-server enable** command in global configuration mode. To disable SNMP, use the **no** form of this command.

snmp-server enable

no snmp-server enable

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the SNMP server is enabled.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This command lets you enable and disable SNMP easily, without having to configure and reconfigure the SNMP traps or other configuration.

Note If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example enables SNMP, configures the SNMP host and traps, and then sends traps as system messages.

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server enable traps

To enable the FWSM to send traps to the NMS, use the **snmp-server enable traps** command in global configuration mode. To disable traps, use the **no** form of this command.

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **cpu threshold** [*trap*] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **nat** [*trap*] | **remote-access** [*trap*] | **resource** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **cpu threshold** [*trap*] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **nat** [*trap*] | **remote-access** [*trap*] | **resource** [*trap*]]

Syntax Description

all	Enables all traps.
cpu threshold [*trap*]	Enables CPU threshold traps. Traps for **cpu threshold** include: • **rising**
entity [*trap*]	Enables entity traps. Traps for **entity** include: • **config-change** • **fru-insert** • **fru-remove** • **redun-switchover** • **alarm-asserted** • **alarm-cleared**
ipsec [*trap*]	Enables IPSec traps. Traps for **ipsec** include: • **start** • **stop**
nat [*trap*]	Enables NAT-related traps. Traps for **nat** include: • **packet-discard**
remote-access [*trap*]	Enables remote access traps. Traps for **remote-access** include: • **session-threshold-exceeded**
resource [*trap*]	Enables resource limit traps. Traps for **resource** include: • **limit-reached** • **rate-limit-reached**
snmp [*trap*]	Enables SNMP traps. By default, all SNMP traps are enabled. Traps for **snmp** include: • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	Enables syslog traps.

Defaults

The default configuration has all **snmp** traps enabled (**snmp-server enable traps snmp authentication linkup linkdown coldstart**). You can disable these traps using the **no** form of this command with the **snmp** keyword. However, the **clear configure snmp-server** command restores the default enabling of SNMP traps.

If you enter this command and do not specify a trap type, then the default is **syslog**. (The default **snmp** traps continue to be enabled along with the **syslog** trap.)

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	Added **cpu threshold** trap: *rising*. Added **entity** traps: *redun-switchover*, *alarm-asserted*, and *alarm-cleared*. Added **nat** trap: *packet-discard*. Added **resource** traps: *limit-reached* and *rate-limit-reached*.
4.0(1)	The **remote-access** option in multi-firewall mode was removed.

Usage Guidelines

Enter this command for each feature type to enable individual traps or sets of traps, or enter the **all** keyword to enable all traps.

To send traps to the NMS, enter the **logging history** command, and enable logging using the **logging enable** command.

The **remote-access** option is not available in multi-firewall mode in FWSM Version 4.0(1).

Note If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example enables SNMP, configures the SNMP host and traps, and then sends traps as system messages.

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the FWSM.
snmp-server host	Sets the SNMP host address.
snmp-server location	Sets the SNMP server location string.

snmp-server host

To specify the NMS that can use SNMP on the FWSM, use the **snmp-server host** command in global configuration mode. To disable the NSM, use the **no** form of this command.

snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

no snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

Syntax Description

community *text*	Sets the community string for this NMS.
host	Specifies an IP address of the NMS to which traps should be sent or from which SNMP requests come.
interface_name	Specifies the interface name through which the NMS communicates with the FWSM.
ip_address	Specifies the IP address of an NMS to which SNMP traps should be sent or from which the SNMP requests come.
trap	(Optional) Specifies that only traps are sent, and that this host is not allowed to browse (poll).
poll	(Optional) Specifies that this host is allowed to browse (poll), but no traps are sent.
udp-port *udp_port*	(Optional) Sets the UDP port to which notifications are sent. SNMP traps are sent on UDP port 162 by default.
version {**1** | **2c**}	(Optional) Sets the SNMP notification version to version 1 or 2c.

Defaults

The default UDP port is 162.

The default version is 1.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You can specify up to 32 NMSs.

Note If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example sets the host to 10.1.2.42 attached to the perimeter interface:

```
hostname(config)# snmp-server host perimeter 10.1.2.42
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the FWSM.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server listen-port

To set the listen port for SNMP requests, use the **snmp-server listen-port** command in global configuration mode. To restore the default port, use the **no** form of the command.

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

Syntax Description

lport	The port on which incoming requests will be accepted. The default port is 161.

Defaults

The default port is 161.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example sets the listen port to 192:

```
hostname(config)# snmp-server listen-port 192
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the FWSM.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server location

To set the FWSM location for SNMP, use the **snmp-server location** command in global configuration mode. To remove the location, use the **no** form of this command.

snmp-server location *text*

no snmp-server location [*text*]

Syntax Description

location *text*	Specifies the security appliance location. 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

If the console access rule limit has been met in NP3, and you try to add an **snmp-server** command, the rule download fails, but the line stays in the running configuration. You can save this setting to the startup configuation so that after a reboot, other console access rule (that is, SSH, Telnet, HTTP, and ICMP) commands are not included in the configuration.

Examples

The following example sets the location as Building 42, Sector 54:

```
hostname(config)# snmp-server location Building 42, Sector 54
```

Related Commands

Command	Description
snmp-server community	Sets the SNMP community string.
snmp-server contact	Sets the SNMP contact name.
snmp-server enable	Enables SNMP on the FWSM.

Command	Description
snmp-server enable traps	Enables SNMP traps.
snmp-server host	Sets the SNMP host address.

software-version

To identify the Server and User-Agent header fields, which expose the software version of either a server or an endpoint, use the **software-version** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

software-version action {**mask** | **log**} [**log**}

no software-version action {**mask** | **log**} [**log**}

Syntax Description

mask	Masks the software version in the SIP message.
log	Specifies standalone or additional log in case of violation.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to identify the software version in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# software-version action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

split-dns

To enter a list of domains to be resolved through the split tunnel, use the **split-dns** command in group-policy configuration mode. To delete a list, use the **no** form of this command.

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

Syntax Description

value *domain-name*	Provides a domain name that the FWSM resolves through the split tunnel.
none	Indicates that there is no split DNS list. Sets a split DNS list with a null value, thereby disallowing a split DNS list. Prevents inheriting a split DNS list from a default or specified group policy.

Defaults

Split DNS is disabled.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use a single space to separate each entry in the list of domains. There is no limit on the number of entries, but the entire string can be no longer than 255 characters. You can use only alphanumeric characters, hyphens (-), and periods (.).

To delete all split tunneling domain lists, use the **no split-dns** command without arguments. This deletes all configured split tunneling domain lists, including a null list created by issuing the **split-dns none** command.

When there are no split tunneling domain lists, users inherit any that exist in the default group policy. To prevent users from inheriting such split tunneling domain lists, use the **split-dns none** command.

Examples

The following example shows how to configure the domains Domain1, Domain2, Domain3 and Domain4 to be resolved through split tunneling for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the FWSM uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form

split-horizon

To reenable EIGRP split horizon, use the **split-horizon** command in interface configuration mode. To disable EIGRP split horizon, use the **no** form of this command.

split-horizon eigrp *as-number*

no split-horizon eigrp *as-number*

Syntax Description

as-number	The autonomous system number of the EIGRP routing process.

Defaults

The **split-horizon** command is enabled.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

For networks that include links over X.25 packet-switched networks, you can use the **neighbor** command to defeat the split horizon feature. As an alternative, you can explicitly specify the **no split-horizon eigrp** command in your configuration. However, if you do so, you must similarly disable split horizon for all routers and access servers in any relevant multicast groups on that network.

In general, it is best that you not change the default state of split horizon unless you are certain that your application requires the change in order to properly advertise routes. If split horizon is disabled on a serial interface and that interface is attached to a packet-switched network, you must disable split horizon for all routers and access servers in any relevant multicast groups on that network.

Examples

The following example disables EIGRP split horizon on interface Vlan10:

```
hostname(config)# interface Vlan10
hostname(config-if)# no split-horizon eigrp 100
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

split-tunnel-network-list

To create a network list for split tunneling, use the **split-tunnel-network-list** command in group-policy configuration mode. To delete a network list, use the **no** form of this command.

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

Syntax Description

value *access-list name*	Identifies an access list that enumerates the networks to tunnel or not tunnel.
none	Indicates that there is no network list for split tunneling; the FWSM tunnels all traffic. Sets a split tunneling network list with a null value, thereby disallowing split tunneling. Prevents inheriting a default split tunneling network list from a default or specified group policy.

Defaults

By default, there are no split tunneling network lists.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM makes split tunneling decisions on the basis of a network list, which is a standard ACL that consists of a list of addresses on the private network.

To delete all split tunneling network lists, use the **no split-tunnel-network-list** command without arguments. This deletes all configured network lists, including a null list created by issuing the **split-tunnel-network-list none** command.

When there are no split tunneling network lists, users inherit any network lists that exist in the default or specified group policy. To prevent users from inheriting such network lists, use the **split-tunnel-network-list none** command.

Split tunneling network lists distinguish networks that require traffic to travel across the tunnel from those that do not require tunneling.

Examples

The following example shows how to set a network list called FirstList for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form.

split-tunnel-policy

To set a split tunneling policy, use the **split-tunnel-policy** command in group-policy configuration mode. To remove the split-tunnel-policy attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for split tunneling from another group policy.

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

Syntax Description

excludespecified	Defines a list of networks to which traffic goes in the clear. This feature is useful for remote users who want to access devices on their local network, such as printers, while they are connected to the corporate network through a tunnel. This option applies only to the Cisco VPN client.
split-tunnel-policy	Indicates that you are setting rules for tunneling traffic.
tunnelall	Specifies that no traffic goes in the clear or to any other destination than the FWSM. Remote users reach internet networks through the corporate network and do not have access to local networks.
tunnelspecified	Tunnels all traffic from or to the specified networks. This option enables split tunneling. It lets you create a network list of addresses to tunnel. Data to all other addresses travels in the clear, and is routed by the Internet service provider of the remote user.

Defaults

Split tunneling is disabled by default, which is tunnelall.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Split tunneling is primarily a traffic management feature, not a security feature. In fact, for optimum security, we recommend that you not enable split tunneling. Split tunneling lets a remote-access IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form. With split-tunneling enabled, packets not bound for destinations on the other side of the IPSec tunnel do not have to be encrypted, sent across the tunnel, decrypted, and then routed to a final destination.

This command applies this split tunneling policy to a specific network.

Examples

The following example shows how to set a split tunneling policy of tunneling only specified networks for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

Related Commands

Command	Description
default-domain	Specifies a default domain name that he IPSec client uses the for DNS queries that omit the domain field.
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list none	Indicates that no access list exists for split tunneling. All traffic travels across the tunnel.
split-tunnel-network-list value	Identifies the access list the FWSM uses to distinguish networks that require tunneling and those that do not.

ssh

To add SSH access to the FWSM, use the **ssh** command in global configuration mode. To disable SSH access to the FWSM, use the **no** form of this command. This command supports IPv4 and IPv6 addresses.

ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address*/*prefix*} *interface*

Syntax Description

interface	The FWSM interface on which SSH is enabled. If not specified, SSH is enabled on all interfaces except the outside interface.
ip_address	IPv4 address of the host or network authorized to initiate an SSH connection to the FWSM. For hosts, you can also enter a host name.
ipv6_address/*prefix*	The IPv6 address and prefix of the host or network authorized to initiate an SSH connection to the FWSM.
mask	Network mask for *ip_address*.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

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

Usage Guidelines

The **ssh** *ip_address* command specifies hosts or networks that are authorized to initiate an SSH connection to the FWSM. You can have multiple ssh commands in the configuration. The **no** form of the command removes a specific SSH command from the configuration. Use the **clear configure ssh** command to remove all SSH commands.

Before you can begin using SSH to the FWSM, you must generate a default RSA key using the **crypto key generate rsa** command.

The following security algorithms and ciphers are supported on the FWSM:

- 3DES and AES ciphers for data encryption
- HMAC-SHA and HMAC-MD5 algorithms for packet integrity
- RSA public key algorithm for host authentication

- Diffie-Hellman Group 1 algorithm for key exchange

The following SSH Version 2 features are not supported on the FWSM:

- X11 forwarding
- Port forwarding
- SFTP support
- Kerberos and AFS ticket passing
- Data compression

Examples

The following example shows how to configure the inside interface to accept SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
crypto key generate rsa	Generates RSA key pairs for identity certificates.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh scopy enable	Enables a secure copy server on the FWSM.
ssh version	Restricts the FWSM to using either SSH Version 1 or SSH Version 2.

ssh disconnect

To disconnect an active SSH session, use the **ssh disconnect** command in privileged EXEC mode.

ssh disconnect *session_id*

Syntax Description

session_id	Disconnects the SSH session specified by the ID number.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You must specify a session ID. Use the **show ssh sessions** command to obtain the ID of the SSH session you want to disconnect.

Examples

The following example shows an SSH session being disconnected:

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

Related Commands

Command	Description
show ssh sessions	Displays information about active SSH sessions to the FWSM.
ssh timeout	Sets the timeout value for idle SSH sessions.

ssh scopy enable

To enable Secure Copy (SCP) on the FWSM, use the **ssh scopy enable** command in global configuration mode. To disable SCP, use the **no** form of this command.

ssh scopy enable

no ssh scopy enable

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

Usage Guidelines

SCP is a server-only implementation; it will be able to accept and terminate connections for SCP but can not initiate them. The FWSM has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the FWSM internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The FWSM license must have the VPN-3DES-AES feature to support SSH version 2 connections.

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the FWSM from the specified client or network.
ssh version	Restricts the FWSM to using either SSH Version 1 or SSH Version 2.

ssh timeout

To change the default SSH session idle timeout value, use the **ssh timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

ssh timeout *number*

no ssh timeout

Syntax Description

number	Specifies the duration in minutes that an SSH session can remain inactive before being disconnected. Valid values are from 1 to 60 minutes.

Defaults

The default session timeout value is 5 minutes.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **ssh timeout** command specifies the duration in minutes that a session can be idle before being disconnected. The default duration is 5 minutes.

Examples

The following example shows how to configure the inside interface to accept only SSH version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
show running-config ssh	Displays the current SSH commands in the running configuration.

Command	Description
show ssh sessions	Displays information about active SSH sessions to the FWSM.
ssh disconnect	Disconnects an active SSH session.

ssh version

To restrict the version of SSH accepted by the FWSM, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command.

ssh version {**1** | **2**}

no ssh version [**1** | **2**]

Syntax Description

1	Specifies that only SSH Version 1 connections are supported.
2	Specifies that only SSH Version 2 connections are supported.

Defaults

By default, both SSH Version 1 and SSH Version 2 are supported.

Command Modes

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

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

Command History

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

Usage Guidelines

1 and 2 specify which version of SSH the FWSM is restricted to using. The **no** form of the command returns the FWSM to the default stance, which is compatible mode (both version can be used). The default values permit SSH Version 1 and SSH Version 2 connections to the FWSM.

Examples

The following example shows how to configure the inside interface to accept SSH Version 2 connections from a management console with the IP address 10.1.1.1. The idle session timeout is set to 60 minutes and SCP is enabled.

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

Related Commands

Command	Description
clear configure ssh	Clears all SSH commands from the running configuration.
debug ssh	Displays debug information and error messages for SSH commands.

Command	Description
show running-config ssh	Displays the current SSH commands in the running configuration.
ssh	Allows SSH connectivity to the FWSM from the specified client or network.

ssl server-version

To specify the SSL/TLS protocol version FWSM uses when acting as a server, use the **ssl server-version** command in global configuration mode. To revert to the default, any, use the **no** version of this command. This command lets you restrict the versions of SSL/TSL that FWSM accepts.

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

Syntax Description

any	Accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3	Accepts SSL version 2 client hellos, and negotiates to SSL version 3.
sslv3-only	Accepts only SSL version 3 client hellos, and uses only SSL version 3.
tlsv1	Accepts SSL version 2 client hellos, and negotiates to TLS version 1.
tlsv1-only	Accepts only TLSv1 client hellos, and uses only TLS version 1.

Defaults

The default value is **any**.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **ssl server-version** command to enforce what version of SSL is accepted when HTTPS clients connect directly to the firewall for management of the firewall. On the FWSM, the command does not support the WebVPN feature.

Examples

The following example shows how to configure FWSM to communicate using only TLSv1 when acting as an SSL server:

```
hostname(config)# ssl server-version tlsv1-only
```

state-checking

To enforce state checking for H.323, use the **state-checking** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

state-checking [h225 | ras]

no state-checking [h225 | ras]

Syntax Description

h225	Enforces state checking for H.225.
ras	Enforces state checking for RAS.

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		
				Multiple	
	Routed	Transparent	Single	Context	System
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to enforce state checking for RAS on an H.323 call:

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# state-checking ras
```

Related Commandsh

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

static

To configure a persistent one-to-one address translation rule by mapping a real IP address to a mapped IP address, use the **static** command in global configuration mode. To restore the default settings, use the **no** form of this command.

For static NAT:

static (*real_ifc*,*mapped_ifc*) {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

no static (*real_ifc*,*mapped_ifc*) {*mapped_ip* | **interface**} {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

For static PAT:

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} {*mapped_ip* | **interface**} *mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name*} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

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**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq**]

Syntax Description

access-list *access_list_name*

Identify the real addresses and destination/source addresses using an extended access list. This feature is known as policy NAT.

Create the extended access list using the **access-list extended** command. The first address in the access list is the real address; the second address is either the source or destination address, depending on where the traffic originates. For example, to translate the real address 10.1.1.1 to the mapped address 192.168.1.1 when 10.1.1.1 sends traffic to the 209.165.200.224 network, the **access-list** and **static** commands are:

```
hostname(config)# access-list TEST extended ip host 10.1.1.1
209.165.200.224 255.255.255.224
hostname(config)# static (inside,outside) 192.168.1.1 access-list TEST
```

In this case, the second address is the destination address. However, the same configuration is used for hosts to originate a connection to the mapped address. For example, when a host on the 209.165.200.224 network initiates a connection to 192.168.1.1, then the second address in the access list is the source address.

This access list should include only **permit** ACEs. You can optionally specify the real and destination ports in the access list using the **eq** operator. Policy NAT and static NAT consider the **inactive** or **time-range** keywords and stop working when an ACE is inactive.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the FWSM translates the .0 and .255 addresses. If you want to prevent access to these addresses, be sure to configure an access list to deny access.

dns

(Optional) Rewrites the A record, or address record, in DNS replies that match this static. For DNS replies traversing from a mapped interface to any other interface, the A record is rewritten from the mapped value to the real value. Inversely, for DNS replies traversing from any interface to a mapped interface, the A record is rewritten from the real value to the mapped value.

emb_lim

(Optional) Specifies the maximum number of embryonic connections per host. The default is 0, which means unlimited embryonic connections.

Limiting the number of embryonic connections protects you from a DoS attack. The FWSM uses the embryonic limit to trigger TCP Intercept, which protects inside systems from a DoS attack perpetrated by flooding an interface with TCP SYN packets. An embryonic connection is a connection request that has not finished the necessary handshake between source and destination.

interface

Uses the interface IP address as the mapped address.

Note You must use the interface keyword instead of specifying the actual IP address when you want to include the IP address of an interface in a static PAT entry.

mapped_ifc

Specifies the name of the interface connected to the mapped IP address network.

mapped_ip

Specifies the address to which the real address is translated.

mapped_port

Specifies the mapped TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 to 65535.

You can view valid port numbers online at the following website:

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

netmask *mask*	Specifies the subnet mask for the real and mapped addresses. For single hosts, use 255.255.255.255. If you do not enter a mask, then the default mask for the IP address class is used, with one exception. If a host-bit is non-zero after masking, a host mask of 255.255.255.255 is used. If you use the **access-list** keyword instead of the *real_ip*, then the subnet mask used in the access list is also used for the *mapped_ip*.
norandomseq	(Optional) Disables TCP ISN randomization protection. TCP initial sequence number randomization can be disabled if another in-line firewall is also randomizing the initial sequence numbers, because there is no need for both firewalls to be performing this action. However, leaving ISN randomization enabled on both firewalls does not affect the traffic. Each TCP connection has two ISNs: one generated by the client and one generated by the server. The security appliance randomizes the ISN of the TCP SYN passing in the outbound direction. If the connection is between two interfaces with the same security level, then the ISN will be randomized in the SYN in both directions. Randomizing the ISN of the protected host prevents an attacker from predecting the next ISN for a new connection and potentially hijacking the new session. 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.
real_ifc	Specifies the name of the interface connected to the real IP address network.
real_ip	Specifies the real address that you want to translate.
real_port	Specifies the real TCP or UDP port. You can specify ports by either a literal name or a number in the range of 0 to 65535. You can view valid port numbers online at the following website: http://www.iana.org/assignments/port-numbers
tcp	For static PAT, specifies the protocol as TCP.
tcp *max_conns*	(Optional) Specifies the maximum number of simultaneous TCP connections allowed to the local host. (See the **local-host** command for more information.) The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The recommended method for setting a connection limit is to use the modular policy framework by setting a connection limit on a class within a policy map.
udp	For static PAT, specifies the protocol as UDP.
udp *udp_max_conns*	(Optional) Specifies the maximum number of simultaneous TCP connections allowed to the local host. (See the **local-host** command for more information.) The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.) The recommended method for setting a connection limit is to use the modular policy framework by setting a connection limit on a class within a policy map.

Defaults

The default value for *tcp_max_conns*, *emb_limit*, and *udp_max_conns* is 0 (unlimited), which is the maximum available.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
2.2(1)	This command was modified to support UDP maximum connections for local hosts.
3.2.(1)	NAT is now supported in transparent firewall mode.

Usage Guidelines

Static NAT creates a fixed translation of real address(es) to mapped address(es).With dynamic NAT and PAT, each host uses a different address or port for each subsequent translation. Because the mapped address is the same for each consecutive connection with static NAT, and a persistent translation rule exists, static NAT allows hosts on the destination network to initiate traffic to a translated host (if there is an access list that allows it).

Note For static policy NAT, in undoing the translation, the ACL in the **static** command is not used. If the destination address in the packet matches the mapped address in the static rule, the static rule is used to untranslate the address.

Matching ports can be used for static policy NAT. Matching ports are not supported for NAT.

The main difference between dynamic NAT and a range of addresses for static NAT is that static NAT allows a remote host to initiate a connection to a translated host (if there is an access list that allows it), while dynamic NAT does not. You also need an equal number of mapped addresses as real addresses with static NAT.

Static PAT is the same as static NAT, except that it lets you specify the protocol (TCP or UDP) and port for the real and mapped addresses.

This feature lets you identify the same mapped address across many different static statements, so long as the port is different for each statement.

You cannot use the same real or mapped address in multiple **static** commands between the same two interfaces, unless you use static PAT. Do not use a mapped address in the **static** command that is also defined in a **global** command for the same mapped interface.

When you specify the ports in policy NAT for applications that require application inspection for secondary channels (FTP, VoIP, and so on), the FWSM automatically translates the secondary ports.

You can alternatively set connection limits (but not embryonic connection limits) using the Modular Policy Framework. See the **set connection** commands for more information. You can only set embryonic connection limits using NAT. If you configure these settings for the same traffic using both methods, then the FWSM uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the FWSM disables TCP sequence randomization.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the FWSM translates the .0 and .255 addresses. If you want to prevent access to these addresses, be sure to configure an access list to deny access.

If you change or remove a **static** command, existing connections that use the translation are not affected. To remove these connections, enter the **clear local-host** or the **clear xlate** command. The **clear xlate** command clears all connections, even when xlate-bypass is enabled and when a connection does not have an xlate.

Examples

Static NAT Examples

For example, the following policy static NAT example shows a single real address that is translated to two mapped addresses depending on the destination address:

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0 255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

The following command maps an inside IP address (10.1.1.3) to an outside IP address (209.165.201.12):

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask 255.255.255.255
```

The following command maps the outside address (209.165.201.15) to an inside address (10.1.1.6):

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask 255.255.255.255
```

The following command statically maps an entire subnet:

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

The following 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 209.165.201.0 through 209.165.201.30 to local addresses 10.1.1.0 through 10.1.1.30 (209.165.201.1 maps to 10.1.1.1, 209.165.201.10 maps to 10.1.1.10, and so on).

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask 255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq h323
hostname(config)# access-group acl_out in interface outside
```

The following example shows the commands that are used to disable Mail Guard:

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

In the example, the **static** command allows you to set up a global address to permit outside hosts access to the 10.1.1.1 mail server host on the dmz1 interface. You shoud set the MX record for DNS to point to the 209.165.201.1 address so that mail is sent to this address. The **access-list** command allows the outside users to access the global address through the SMTP port (25). The **no fixup protocol** command disables Mail Guard.

Static PAT Examples

For example, for Telnet traffic initiated from hosts on the 10.1.3.0 network to the FWSM outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering the following commands:

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 10.1.3.0 255.255.255.0 eq
telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

For HTTP traffic initiated from hosts on the 10.1.3.0 network to the FWSM outside interface (10.1.2.14), you can redirect the traffic to the inside host at 10.1.1.15 by entering:

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 10.1.3.0 255.255.255.0 eq
http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

To redirect Telnet traffic from the FWSM outside interface (10.1.2.14) to the inside host at 10.1.1.15, enter the following command:

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
```

If you want to allow the preceding real Telnet server to initiate connections, though, then you need to provide additional translation. For example, to translate all other types of traffic, enter the following commands. The original **static** command provides translation for Telnet to the server, while the **nat** and **global** commands provide PAT for outbound connections from the server.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

If you also have a separate translation for all inside traffic, and the inside hosts use a different mapped address from the Telnet server, you can still configure traffic initiated from the Telnet server to use the same mapped address as the **static** statement that allows Telnet traffic to the server. You need to create a more exclusive **nat** statement just for the Telnet server. Because **nat** statements are read for the best match, more exclusive **nat** statements are matched before general statements. The following example shows the Telnet **static** statement, the more exclusive **nat** statement for initiated traffic from the Telnet server, and the statement for other inside hosts, which uses a different mapped address.

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet netmask
255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

To translate a well-known port (80) to another port (8080), enter the following command:

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

Related Commands

Command	Description
clear configure static	Removes **static** commands from the configuration.
clear xlate	Clears all translations.
nat	Configures dynamic NAT.

Command	Description
show running-config static	Displays all **static** commands in the configuration.
timeout conn	Sets the timeout for connections.

strict-header-validation

To enable strict validation of the header fields in the SIP messages according to RFC 3261, use the **strict-header-validation** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**]

no strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**]

Syntax Description

drop	Drops the packet if validation occurs.
drop-connection	Drops the connection of a violation occurs.
reset	Resets the connection when a violation occurs.
log	Specifies standalone or additional log when a violation occurs. It can be associated to any of the actions.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

To send a TCP reset from the universal access concentrator (UAC) to the user agent server (UAS) when there is a violation in SIP message header, you must configure the **service resetinbound** command in addition to entering the **reset log** keywords for the **strict-header-validation** command.

When the security level is different on the inside and outside interfaces, the reset is sent to the inside host only. To send the reset to the outside, you must configure the **service resetinbound** command and enter the **reset log** keywords for the **strict-header-validation** command.

Examples

The following example shows how to enable strict validation of SIP header fields in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# strict-header-validation action log
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

strict-http

To allow forwarding of non-compliant HTTP traffic, use the **strict-http** command in HTTP map configuration mode, which is accessible using the **http-map** command. To reset this feature to its default behavior, use the **no** form of the command.

strict-http action {**allow** | **reset** | **drop**} [**log**]

no strict-http action {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	The action taken when a message fails this command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generate a syslog.
reset	Closes the connection with a TCP reset message to client and server.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the FWSM to allow forwarding of non-compliant HTTP traffic. This command overrides the default behavior, which is to deny forwarding of non-compliant HTTP traffic.

Examples

The following example allows forwarding of non-compliant HTTP traffic:

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
```

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.

strip-group

This command applies only to usernames received in the form user@realm. A realm is an administrative domain appended to a username with the @ delimiter (juser@abc).

To enable or disable strip-group processing, use the **strip-group** command in tunnel-group general-attributes mode. The FWSM selects the tunnel group for PPP connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the FWSM sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the FWSM sends the entire username including the realm.

To disable strip-group processing, use the **no** form of this command.

strip-group

no strip-group

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPSec remote access and L2TP/IPSec tunnel-type.

Examples

The following example configures a remote access tunnel group named “remotegrp” for type IPSec remote access, then enters general configuration mode, sets the tunnel group named “remotegrp” as the default group policy, and then enables strip group for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-group
hostname(config-general)
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
group-delimiter	Enables group-name parsing and specifies the delimiter to be used when parsing group names from the user names that are received when tunnels are being negotiated.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default group	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

strip-realm

To enable or disable strip-realm processing, use the **strip-realm** command in tunnel-group general-attributes configuration mode. Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. A realm is an administrative domain appended to a username with the @ delimiter (username@realm). If the command is enabled, the FWSM sends only the user part of the username authorization/authentication. Otherwise, the FWSM sends the entire username.

To disable strip-realm processing, use the **no** form of this command.

strip-realm

no strip-realm

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting for this command is disabled.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can apply this attribute only to the IPSec remote access tunnel-type.

Examples

The following example configures a remote access tunnel group named "remotegrp" for type IPSec remote access, then enters general configuration mode, sets the tunnel group named "remotegrp" as the default group policy, and then enables strip realm for that tunnel group:

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# strip-realm
```

```
neral)
ostname(config-ge
```

Related Commandsh

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

subject-name (crypto ca certificate map)

To indicate that rule entry is applied to the subject DN of the IPSec peer certificate, use the **subject-name** command in CA certificate map configuration mode. To remove a subject-name, use the **no** form of the command.

subject-name [**attr** *tag*] {**eq** | **ne** | **co** | **nc**} *string*

no subject-name [**attr** *tag*] {**eq** | **ne** | **co** | **nc**} *string*

Syntax Description

attr *tag*	IOptional) Indicates that only the specified attribute value from the certificate DN will be compared to the rule entry string. The tag values are as follows:
	DNQ = DN qualifier
	GENQ = Generational qualifier
	I = Initials
	GN = Given name
	N = Name
	SN = Surname
	IP = IP address
	SER = Serial number
	UNAME = Unstructured name
	EA = Email address
	T = Title
	O = Organization Name
	L = Locality
	SP = State/Province
	C = Country
	OU = Organizational unit
	CN = Common name

co	Specifies that the rule entry string must be a substring in the DN string or indicated attribute.
eq	Specifies that the DN string or indicated attribute must match the entire rule string.
nc	Specifies that the rule entry string must not be a substring in theDN string or indicated attribute.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
string	Specifies the value to be matched.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters the CA certificate map mode for certificate map 1 and creates a rule entry indicating that the Organization attribute of the certificate subject name must be equal to Central.

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
hostname(config)#
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
issuer-name	Identifies the DN from the CA certificate that is to be compared to the rule entry string.
tunnel-group-map	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

subject-name (crypto ca trustpoint)

To include the indicated subject DN in the certificate during enrollment, use the **subject-name** command in crypto ca trustpoint configuration mode. This is the person or system that uses the certificate. To restore the default setting, use the **no** form of the command.

subject-name *X.500_name*

no subject-name

Syntax Description

X.500_name	Defines the X.500 distinguished name, for example: cn=crl,ou=certs,o=CAName,c=US. The maximum length is 1K characters (effectively unbounded).

Defaults

The default setting is not to include the subject name.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and sets up automatic enrollment at the URL https//:www.example.com and includes the subject DN OU cisco.example in the the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://www.example.com/
hostname(ca-trustpoint)# subject-name ou=cisco.example
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment url	Specifies the URL for enrolling with a CA.

summary-address eigrp

To configure a summary for EIGRP on a specific interface, use the **summary-address eigrp** command in interface configuration mode. To remove the summary address, use the **no** form of this command.

summary-address eigrp *as-number addr mask* [*admin-distance*]

no summary-address *as-number addr mask*

Syntax Description

as-number	The autonomous system number. This must be the same as the autonomous system number of your EIGRP routing process.
addr	The summary IP address.
mask	The subnet mask to apply to the IP address.
admin-distance	(Optional) The administrative distance of the summary route. Valid values are from 0 to 255. If not specified, the default value is 5.

Defaults

The defaults are as follows:

- EIGRP automatically summarizes routes to the network level, even for a single host route.
- The administrative distance of EIGRP summary routes is 5.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

By default, EIGRP summarizes subnet routes to the network level. Use the **no auto-summary** command to disable automatic route summarization. Using the **summary-address eigrp** command lets you manually define subnet route summaries on a per-interface basis.

Examples

The following example configures route summarization with a **tag** set to 3:

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

The following example removes the **summary-address** command from the configuration:

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

Related Commands

Command	Description
auto-summary	Automatically creates summary addresses for the EIGRP routing process.

summary-address

To create aggregate addresses for OSPF, use the **summary-address** command in router configuration mode. To remove the summary address or specific summary address options, use the **no** form of this command.

summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

no summary-address *addr mask* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

addr	Value of the summary address that is designated for a range of addresses.
mask	IP subnet mask that is used for the summary route.
not-advertise	(Optional) Suppresses routes that match the specified prefix/mask pair.
tag *tag_value*	(Optional) A 32-bit decimal value attached to each external route. This value is not used by OSPF itself. It may be used to communicate information between ASBRs. If none is specified, then the remote autonomous system number is used for routes from BGP and EGP; for other protocols, zero (0) is used. Valid values range from 0 to 4294967295.

Defaults

The defaults are as follows:

- *tag_value* is 0.
- Routes that match the specified prefix/mask pair are not suppressed.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Routes learned from other routing protocols can be summarized. Using this command for OSPF causes an OSPF Autonomous System Boundary Router (ASBR) to advertise one external route as an aggregate for all redistributed routes that are covered by the address. This command summarizes only routes from other routing protocols that are being redistributed into OSPF. Use the **area range** command for route summarization between OSPF areas.

To remove a **summary-address** command from the configuration, use the no form of the command without specifying any of the optional keywords or arguments. To remove an option from a summary command in the configuration, use the **no** form of the command with the options that you want removed. See the "Examples" section for more information.

Examples

The following example configures route summarization with a **tag** set to 3:

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

The following example shows how to use the **no** form of the **summary-address** command with an option to set that option back to the default value. In this example, the **tag** value, set to 3 in the previous example, is removed from the **summary-address** command.

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

The following example removes the **summary-address** command from the configuration:

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

Related Commands

Command	Description
area range	Consolidates and summarizes routes at an area boundary.
router ospf	Enters router configuration mode.
show ospf summary-address	Displays the summary address settings for each OSPF routing process.

sunrpc-server

To create entries in the SunRPC services table, use the **sunrpc-server** command in global configuration mode. To remove SunRPC services table entries from the configuration, use the **no** form of this command.

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **{protocol** {**tcp** | **udp**}} **port** *port* **[-** *port* **] timeout** *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **{protocol** {**tcp** | **udp**}} **port** *port* [- *port]* **timeout** *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

Syntax Description

ifc_name	Server interface name.
ip_addr	SunRPC server IP address.
mask	Network mask.
port *port* [- *port*]	Specifies the SunRPC protocol port range.
protocol tcp	Specifies the SunRPC transport protocol.
protocol udp	Specifies the SunRPC transport protocol.
service *service_type*	Sets the SunRPC service program number as specified in the output of a SunOS **rpcinfo** command.
timeout *hh:mm:ss*	Specifies the timeout idle time after which the access for the SunRPC service traffic is closed.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	The **rpc-server** command was introduced.
3.1(1)	This command was changed from **rpc-server**.

Usage Guidelines

The SunRPC services table is used to allow SunRPC traffic through the FWSM based on an established SunRPC session for the duration specified by the timeout.

Examples

The following examples show how to create an SunRPC services table.

```
hostname(config)# sunrpc-server outside 10.10.10.10 255.255.255.255 service 100003
protocol TCP port 111 timeout 0:10:00
hostname(config)# sunrpc-server outside 10.10.10.0 255.255.255.0 service 100003 protocol
TCP port 111 timeout 0:10:00
```

In the first example, *ip_addr* contains the IP address of the server host; therefore, the netmask should be 255.255.255.255. In the second example, *ip_addr* contains the network IP address of the server: therefore, the netmask should be 255.255.255.0.

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the FWSM.
show running-config sunrpc-server	Displays the information about the SunRPC configuration.

support-user-cert-validation

To validate a remote user certificate based on the current trustpoint, provided that this trustpoint is authenticated to the CA that issued the remote certificate, use the **support-user-cert-validation** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

support-user-cert-validation

no support-user-cert-validation

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to support user certificate validation.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM can have two trustpoints with the same CA resulting in two different identity certificates from the same CA. This option is automatically disabled if the trustpoint is authenticated to a CA that is already associated with another trustpoint that has enabled this feature. This prevents ambiguity in the choice of path-validation parameters. If the user attempts to activate this feature on a trustpoint that has been authenticated to a CA already associated with another trustpoint that has enabled this feature, the action is not permitted. No two trustpoints can have this setting enabled and be authenticated to the same CA.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and enables the trustpoint central to accept user validation:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

Related Commands

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

sysopt connection tcpmss

To ensure that the maximum TCP segment size does not exceed the value you set and that the maximum is not less than a specified size, use the **sysopt connection tcpmss** command in global configuration mode. To restore the default setting, use the **no** form of this command.

sysopt connection tcpmss [**minimum**] *bytes*

no sysopt connection tcpmss [**minimum**] [*bytes*]

Syntax Description

bytes	Sets the maximum TCP segment size in bytes, between 48 and any maximum number. The default value is 1380 bytes. You can disable this feature by setting *bytes* to 0. For the **minimum** keyword, the *bytes* represent the smallest maximum value allowed.
minimum	(Optional) Overrides the maximum segment size to be no less than *bytes*, between 48 and 65535 bytes. This feature is disabled by default (set to 0).

Defaults

The default maximum value is 1380 bytes. The minimum feature is disabled by default (set to 0).

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Both the host and the server can set the maximum segment size when they first establish a connection. If either maximum exceeds the value you set with the **sysopt connection tcpmss** command, then the FWSM overrides the maximum and inserts the value you set. If either maximum is less than the value you set with the **sysopt connection tcpmss minimum** command, then the FWSM overrides the maximum and inserts the "minimum" value you set (the minimum value is actually the smallest maximum allowed). For example, if you set a maximum size of 1200 bytes and a minimum size of 400 bytes, when a host requests a maximum size of 1300 bytes, then the FWSM alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the FWSM alters the packet to request 400 bytes (the minimum).

The default of 1380 bytes allows room for header information so that the total packet size does not exceed 1500 bytes, which is the default MTU for Ethernet. See the following calculation:

1380 data + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1500 bytes

If the host or server does not request a maximum segment size, the FWSM assumes that the RFC 793 default value of 536 bytes is in effect.

If you set the maximum size to be greater than 1380, packets might become fragmented, depending on the MTU size (which is 1500 by default). Large numbers of fragments can impact the performance of the FWSM when it uses the Frag Guard feature. Setting the minimum size prevents the TCP server from sending many small TCP data packets to the client and impacting the performance of the server and the network.

Note Although not advised for normal use of this feature, if you encounter the syslog IPFRAG messages 209001 and 209002, you can raise the *bytes* value.

Examples

The following example sets the maximum size to 1200 and the minimum to 400:

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

sysopt connection tcp sack-permitted

To allow the Selective-ACK-Permitted option (type 4) exchanged during the TCP 3-way handshake, use the **sysopt connection tcp sack-permitted** command in global configuration mode. To clear the Selective-ACK-Permitted option, use the **no** form of this command. Because the FWSM does not support the Selective-ACK option (type 5) in TCP packets, the **no** form of this command prevents the sender from including the SACK option in packets.

sysopt connection tcp sack-permitted

no sysopt connection tcp sack-permitted

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default, and the Selective-ACK-Permitted option remains intact.

Command Modes

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

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

Command History

Release	Modification
3.2(8)/4.0(3)	This command was introduced.

Usage Guidelines

The FWSM does not support the Selective-ACK option (type 5). If the Selective-ACK option is enabled in a connection where sequence number randomization is enabled (the default), then you might see poor performance because the FWSM does not properly adjust the sequence numbers present inside the Selective-ACK option according to the randomized sequence. For example, the data sender unnecessarily retransmits segments that have been correctly received.

To prevent the receipt of packets with the Selective-ACK option, the **no sysopt connection tcp sack-permitted** command disables the Selective-ACK negotiation during the handshake by clearing the Selective-ACK-Permitted option. The FWSM will replace the Selective-ACK-Permitted option with no operation (NOP) option, without changing the total length of the packet. Using the **no** form of this command prevents unnecessary retransmissions, and prevents you from having to disable Initial Sequence Number (ISN) randomization.

Examples

The following example clears the Selective-ACK-Permitted option:

```
hostname(config)# no sysopt connection tcp sack-permitted
```

Related Commands

Command	Description
sysopt connection tcpmss	Ensures that the maximum TCP segment size does not exceed the value you set and that the maximum is not less than a specified size.

sysopt connection tcp window-scale

To allow the TCP window-scale option, use the **sysopt connection tcp window-scale** command in global configuration mode. To replace the TCP window scale option with the no operation (NOP) option,without changing the total length of the packet, use the **no** form of this command.

sysopt connection tcp window-scale

no sysopt connection tcp window-scale

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(8)/3.2(5)	This command was introduced.

Usage Guidelines

You should disable this command if you want to disable window scaling. For example, certain inspection engines (SIP, Skinny) use TCP Proxy to reassemble the application payload spanning multiple TCP segments. The TCP Proxy is unaware of TCP Window Scaling options on the segments, and it is unable to reassemble such flows correctly unless you disable window scaling.

Examples

The following example disables window scaling:

```
hostname(config)# no sysopt connection tcp window-scale
```

Related Commands

Command	Description
sysopt connection tcpmss	Ensures that the maximum TCP segment size does not exceed the value you set and that the maximum is not less than a specified size.
sysopt connection tcp sack-permitted	Allows the Selective-ACK-Permitted option (type 4) exchanged during the TCP 3-way handshake.

Related Commands

sysopt connection udp create-arp-unresolved-conn

To create UDP sessions in the accelerated path with a "pending for ARP" state, use the **sysopt connection udp create-arp-unresolved-conn** command in global configuration mode. To use the default behavior, where the accelerated path rejects the session when there is no ARP entry, use the **no** form of this command. If you configure the FWSM to create the session in the accelerated path even though the ARP lookup fails, then it will drop all further packets to the destination IP address until the ARP lookup succeeds. Without this command, each subsequent UDP packet goes through the session management path before being dropped by the accelerated path, causing potential overload of the session management path.

sysopt connection udp create-arp-unresolved-conn

no sysopt connection udp create-arp-unresolved-conn

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
4.1(1)	This command was introduced.

Usage Guidelines

When you enable the **sysopt connection udp create-arp-unresolved-conn** command, UDP packets are treated as follows:

1. The FWSM receives a UDP packet that does not have a session in the accelerated path. Therefore, the packet is sent through the session management path.
2. In the session management path, all the rules (access list, NAT, etc.) are applied.
3. If the packet is permitted, the session management path inserts a session in the accelerated path.

Note If the packet is denied, the session management path drops it. The **sysopt connection udp create-arp-unresolved-conn** command only affects permitted packets.

4. If the accelerated path does not have an ARP entry for the destination IP address in this packet, it initiates an ARP request on the destination interface. Meanwhile, it creates the session with a "pending for ARP" tag. While the "pending for ARP" tag is present, all packets in this session are dropped, including the initial packet.
5. Depending on the status of the ARP lookup, the following situations can occur:

- If the ARP response is received, the "pending for ARP" tag is removed, and packets are now allowed through for this session.
- If the ARP query times-out, this session is maintained with the "pending for ARP" tag, and packets continue to be dropped until the session times-out or is cleared through other means.

If you do not enable the **sysopt connection udp create-arp-unresolved-conn** command, UDP packets with a failed ARP lookup are denied a session by the accelerated path, and it drops the packet. Because there is no session in the accelerated path, subsequent packets to the same IP address continue to go through the sesssion management path, and are again dropped by the accelerated path. Only if the ARP lookup succeeds will the session be established in the accelerated path.

Examples

The following example enables UDP sessions in the accelerated path when the ARP lookup fails:

```
hostname(config)# sysopt connection udp create-arp-unresolved-conn
```

Related Commands

Command	Description
sysopt connection tcpmss	Ensures that the maximum TCP segment size does not exceed the value you set and that the maximum is not less than a specified size.
sysopt connection tcp sack-permitted	Allows the Selective-ACK-Permitted option (type 4) exchanged during the TCP 3-way handshake.

sysopt nodnsalias

To disable DNS inspection that alters the DNS A record address when you use the **alias** command, use the **sysopt nodnsalias** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to disable DNS application inspection if you want the **alias** command to perform only NAT, and DNS packet alteration is undesirable.

sysopt nodnsalias {**inbound** | **outbound**}

no sysopt nodnsalias {**inbound** | **outbound**}

Syntax Description

inbound	Disables DNS record alteration for packets from lower security interfaces to higher security interfaces specified by an **alias** command.
outbound	Disables DNS record alteration for packets from higher security interfaces specified by an **alias** command to lower security interfaces.

Defaults

This feature is disabled by default (DNS record address alteration is enabled).

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The **alias** command performs NAT and DNS A record address alteration. In some cases, you might want to disable the DNS record alteration.

Examples

The following example disables the DNS address alteration for inbound packets:

```
hostname(config)# sysopt nodnsalias inbound
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.

Command	Description
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt noproxyarp	Disables proxy ARP on an interface.

sysopt noproxyarp

To disable proxy ARP for NAT global addresses on an interface, use the **sysopt noproxyarp** command in global configuration mode. To reenable proxy ARP for global addresses, use the **no** form of this command.

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

Syntax Description

interface_name	Specifies the interface name for which you want to disable proxy ARP.

Defaults

Proxy ARP for global addresses is enabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

In rare circumstances, you might want to disable proxy ARP for global addresses.

When a host sends IP traffic to another device on the same Ethernet network, the host needs to know the MAC address of the device. ARP is a Layer 2 protocol that resolves an IP address to a MAC address. A host sends an ARP request asking “Who is this IP address?” The device owning the IP address replies, “I own that IP address; here is my MAC address.”

Proxy ARP is when a device responds to an ARP request with its own MAC address, even though the device does not own the IP address. The FWSM uses proxy ARP when you configure NAT and specify a global address that is on the same network as the FWSM interface. The only way traffic can reach the hosts is if the FWSM uses proxy ARP to claim that the FWSM MAC address is assigned to destination global addresses.

Examples

The following example disables proxy ARP on the inside interface:

```
hostname(config)# sysopt noproxyarp inside
```

Related Commands

Command	Description
alias	Translates an outside address and alters the DNS records to accommodate the translation.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt nodnsalias	Disables alteration of the DNS A record address when you use the **alias** command.

sysopt np completion-unit

To enable the hardware completion unit in the accelerated path network processors (NPs), which ensures that packets are forwarded out in the same order they were received in the ingress queues of the NPs., use the **sysopt np completion-unit** command in global configuration mode. To restore the default setting, use the **no** form of this command.

sysopt np completion-unit

no sysopt np completion-unit

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	• (Admin only)	—

Command History

Release	Modification
3.2(5)	This command was introduced.

Usage Guidelines

When you enable this command in the admin context, it is enabled for the whole device. You cannot configure this command separately for each context.

Because of design constraints:

- This command only works for packets forwarded by the accelerated path. Packets that require inspection, for example, go through the session management path or the control path, and are not affected by this command.
- This command does not guarantee that the order of multicast packets are maintained in routed mode
- This command does not guarantee the order of fragmented packets or packets to be fragmented by the FWSM because of its MTU.
- Do not enable this command when the FWSM is oversubscribed. This command enables additional processing in NP1 and NP2. Over-subscription will contribute to packets being dropped that are not reported by syslogs.

Examples

The following example enables the hardware completion unit:

```
hostname(config)# sysopt np completion-unit
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

sysopt radius ignore-secret

To ignore the authentication key in RADIUS accounting responses, use the **sysopt radius ignore-secret** command in global configuration mode. To disable this feature, use the **no** form of this command. You might need to ignore the key for compatibility with some RADIUS servers.

sysopt radius ignore-secret

no sysopt radius ignore-secret

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Some RADIUS servers, such as Livingston Version 1.16, have a usage caveat where they do not include the key in the authenticator hash in the accounting acknowledgment response. This situation can cause the FWSM to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to ignore the key in the authenticator of accounting acknowledgments thus avoiding the retransmit problem. (The key described here is the key you set with the **aaa-server host** command.)

Examples

The following example ignores the authentication key in accounting responses:

```
hostname(config)# sysopt radius ignore-secret
```

Related Commands

Command	Description
aaa-server host	Identifies a AAA server.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.

sysopt uauth allow-http-cache

To let the web browser supply a username and password from its cache when it reauthenticates with the virtual HTTP server on the FWSM (see the **virtual http** command), use the **sysopt uauth allow-http-cache** command in global configuration mode. If you do not allow the HTTP cache, then after your authentication session times out, the next time you connect to the virtual HTTP server, you are prompted again for your username and password. To disable this feature, use the **no** form of this command.

sysopt uauth allow-http-cache

no sysopt uauth allow-http-cache

Syntax Description

This command has no arguments or keywords.

Defaults

This feature is disabled by default.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example allows the HTTP cache to be used:

```
hostname(config)# sysopt uauth allow-http-cache
```

Related Commands

Command	Description
virtual http	When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command allows you to authenticate separately with the FWSM and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.