CHAPTER 31

shun through sysopt radius ignore-secret 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 security appliance 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 security appliance 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 security appliance connection table and also prevents all future packets from 10.1.1.27 from going through the security appliance.

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
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

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.

Note This command only disables the software interface. The physical link remains up, and the directly connected device is still recognized as being up even when the corresponding interface is configured with the **shutdown** command.

Examples\

The following example enables a main interface:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
```

```
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

The following example enables a subinterface:

```
hostname(config)# interface gigabitethernet0/2.1
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 gigabitethernet0/2.1
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.

sla monitor

To create an SLA operation, use the **sla monitor** command in global configuration mode. To remove the SLA operation, use the **no** form of this command.

sla monitor *sla_id*

no sla monitor *sla_id*

Syntax Description

sla_id	Specifies the ID of the SLA being configured. If the SLA does not already exist, it is created. Valid values are from 1 to 2147483647.

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
7.2(1)	This command was introduced.

Usage Guidelines

The **sla monitor** command creates SLA operations and enters SLA Monitor configuration mode. Once you enter this command, the command prompt changes to `hostname(config-sla-monitor)#` to indicate that you are in SLA Monitor configuration mode. If the SLA operation already exists, and a type has already been defined for it, then the prompt appears as `hostname(config-sla-monitor-echo)#`. You can create a maximum of 2000 SLA operations. Only 32 SLA operations may be debugged at any time.

The **no sla monitor** command removes the specified SLA operation and the commands used to configure that operation.

After you configure an SLA operation, you must schedule the operation with the **sla monitor schedule** command. You cannot modify the configuration of the SLA operation after scheduling it. To modify the the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

To display the current configuration settings of the operation, use the **show sla monitor configuration** command. To display operational statistics of the SLA operation, use the **show sla monitor operation-state command**. To see the SLA commands in the configuration, use the **show running-config sla monitor** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA:

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
frequency	Specifies the rate at which the SLA operation repeats.
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor schedule	Schedules the SLA operation.
timeout	Sets the amount of time the SLA operation waits for a response.
track rtr	Creates a tracking entry to poll the SLA.

sla monitor schedule

To schedule an SLA operation, use the **sla monitor schedule** command in global configuration mode. To remove SLA operation schedule, and place the operation in the pending state, use the **no** form of this command.

sla monitor schedule *sla-id* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no sla monitor schedule *sla-id*

Syntax Description

after *hh*:*mm*:*ss*	Indicates that the operation should start the specified number of hours, minutes, and seconds after the command was entered.
ageout *seconds*	(Optional) Specifies the number of seconds to keep the operation in memory when it is not actively collecting information. After an SLA operation ages out, it is removed from the running configuration.
day	Number of the day to start the operation on. Valid values are from 1 to 31. If a day is not specified, then the current day is used. If you specify a day you must also specify a month.
hh:*mm*[:*ss*]	Specifies an absolute start time in 24-hour notation. Seconds are optional. The next time the specified time occurs is implied unless you specify a *month* and a *day*.
life forever	(Optional) Schedules the operation to run indefinitely.
life *seconds*	(Optional) Sets the number of seconds the operation actively collects information.
month	(Optional) Name of the month to start the operation in. If a month is not specified, then the current month is used. I f you specify a month you must also specify a day. You can enter the full English name of the month or just the first three letters.
now	Indicates that the operation should start as soon as the command is entered.
pending	Indicates that no information is collected. This is the default state.
recurring	(Optional) Indicates that the operation will start automatically at the specified time and for the specified duration every day.
sla-id	The ID of the SLA operation being scheduled.
start-time	Sets the time when the SLA operation starts.

Defaults

The defaults are as follows:

- SLA operations are in the **pending** state until the scheduled time is met. This means that the operation is enabled but not actively collecting data.
- The default **ageout** time is 0 seconds (never ages out).
- The default **life** is 3600 seconds (one hour).

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
7.2(1)	This command was introduced.

Usage Guidelines

When an SLA operation is in an active state, it immediately begins collecting information. The following time line shows the age-out process of the operation:

```
W----------------------X----------------------Y----------------------Z
```

- W is the time the SLA operation was configured with the **sla monitor** command.
- X is the start time of the SLA operation. This is when the operation became "active".
- Y is the end of life as configured with the **sla monitor schedule** command (the **life** seconds have counted down to zero).
- Z is the age out of the operation.

The age out process, if used, starts counting down at W, is suspended between X and Y, and is reset to its configured size are starts counting down again at Y. When an SLA operation ages out, the SLA operation configuration is removed from the running configuration. It is possible for the operation to age out before it executes (that is, Z can occur before X). To ensure that this does not happen, the difference between the operation configuration time and start time (X and W) must be less than the age-out seconds.

The **recurring** keyword is only supported for scheduling single SLA operations. You cannot schedule multiple SLA operations using a single **sla monitor schedule** command. The **life** value for a recurring SLA operation should be less than one day. The **ageout** value for a recurring operation must be "never" (which is specified with the value 0), or the sum of the **life** and **ageout** values must be more than one day. If the recurring option is not specified, the operations are started in the existing normal scheduling mode.

You cannot modify the configuration of the SLA operation after scheduling it. To modify the configuration of a scheduled SLA operation, you must use the **no sla monitor** command to remove the selected SLA operation completely. Removing an SLA operation also removes the associated **sla monitor schedule** command. Then you can reenter the SLA operation configuration.

Examples

The following example shows SLA operation 25 scheduled to begin actively collecting data at 3:00 p.m. on April 5. This operation will age out after 12 hours of inactivity. When this SLA operation ages out, all configuration information for the SLA operation is removed from the running configuration.

```
hostname(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout 43200
```

The following example shows SLA operation 1 schedule to begin collecting data after a 5-minute delay. The default life of one hour applies.

```
hostname(config)# sla monitor schedule 1 start after 00:05:00
```

The following example shows SLA operation 3 scheduled to begin collecting data immediately and is scheduled to run indefinitely:

```
hostname(config)# sla monitor schedule 3 life forever start-time now
```

The following example shows SLA operation 15 scheduled to begin automatically collecting data every day at 1:30 a.m.:

```
hostname(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

Related Commands

Command	Description
show sla monitor configuration	Displays the SLA configuration settings.
sla monitor	Defines an SLA monitoring operation.

smtps

To enter SMTPS configuration mode, use the **smtps** command in global configuration mode. To remove any commands entered in SMTPS command mode, use the **no** version of this command. SMTPS is a TCP/IP protocol that lets you to send e-mail over an SSL connection.

smtps

no smtps

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enter SMTPS configuration mode:

```
hostname(config)# smtps
hostname(config-smtps)#
```

Related Commands

Command	Description
clear configure smtps	Removes the SMTPS configuration.
show running-config smtps	Displays the running configuration for SMTPS.

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 security appliance 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 security appliance.

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
7.0(1)	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
```

Related Commands

Command	Description

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
7.0(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)#
```

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
Preexisting	This command was preexisting.

Usage Guidelines

The SNMP community string is a shared secret among the SNMP management station and the network nodes being managed. The security appliance 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, security appliance, and the management station with this same string. The security appliance uses this string and does not respond to requests with an invalid community string.

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 security appliance.
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 security appliance 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
Preexisting	This command was preexisting.

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 security appliance.
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

To enable the SNMP server on the security appliance, 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
7.0(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.

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.

Command	Description
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 security appliance 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*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

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

Syntax Description

all	Enables all traps.
entity [*trap*]	Enables entity traps. Traps for **entity** include: • **config-change** • **fru-insert** • **fru-remove**
ipsec [*trap*]	Enables IPSec traps. Traps for **ipsec** include: • **start** • **stop**
remote-access [*trap*]	Enables remote access traps. Traps for remote-access include: • **session-threshold-exceeded**
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	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

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.

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 security appliance.
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 security appliance, 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 security appliance.
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
Preexisting	This command was preexisting.

Usage Guidelines

You can specify up to 32 NMSs.

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 security appliance.
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.[1]

1. The **snmp-server listen-port** command is only available in admin context because the command is not available in the system context.

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
Preexisting	This command was preexisting.

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 security appliance.
snmp-server enable traps	Enables SNMP traps.
snmp-server location	Sets the SNMP server location string.

snmp-server location

To set the security appliance 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
Preexisting	This command was preexisting.

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 security appliance.
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
7.2(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.

speed

To set the speed of a copper (RJ-45) Ethernet interface, use the **speed** command in interface configuration mode. To restore the speed setting to the default, use the **no** form of this command.

speed {**auto** | **10** | **100** | **1000** | **nonegotiate**}

no speed [**auto** | **10** | **100** | **1000** | **nonegotiate**]

Syntax Description

10	Sets the speed to 10BASE-T.
100	Sets the speed to 100BASE-T.
1000	Sets the speed to 1000BASE-T. For copper Gigabit Ethernet only.
auto	Auto detects the speed.
nonegotiate	For fiber interfaces, sets the speed to 1000 Mbps and does not negotiate link parameters. This command and the **no** form of this command are the only settings available for fiber interfaces. When you set the value to **no speed nonegotiate** (the default), the interface enables link negotiation, which exchanges flow-control parameters and remote fault information.

Defaults

For copper interfaces, the default is **speed auto**.

For fiber interfaces, the default is **no speed nonegotiate**.

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
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines

Set the speed on the physical interface only.

If your network does not support auto detection, set the speed to a specific value.

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the speed to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Examples

The following example sets the speed to 1000BASE-T:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
duplex	Sets the duplex mode.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.

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.

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.

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 security appliance 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
7.0(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 (.).

The **no split-dns** command, when used without arguments, deletes all current values, including a null value created by issuing the **split-dns none** command.

Neither the AnyConnect VPN client nor the SSL VPN Client supports split DNS.

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 security appliance 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-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.

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.

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 security appliance 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
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance 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.

The **no split-tunnel-network-list** command, when used without arguments, deletes all current network lists, including a null value created by issuing the **split-tunnel-network-list none** command.

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 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.

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 security appliance. 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 remote user's internet service provider.

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
7.0(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.

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 security appliance uses to distinguish networks that require tunneling and those that do not.

spoof-server

To substitute a string for the server header field for HTTP protocol inspection, use the **spoof-server** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

spoof-server *string*

no spoof-server *string*

Syntax Description

string	String to substitute for the server header field. 82 characters maximum.

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
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

WebVPN streams are not subject to the **spoof-server** comand.

Examples

The following example shows how to substitute a string for the server header field in an HTTP inspection policy map:

```
hostname(config-pmap-p)# spoof-server string
```

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.

ssh

To add SSH access to the security appliance, use the **ssh** command in global configuration mode. To disable SSH access to the security appliance, 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 security appliance 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 security appliance. 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 security appliance.
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
Preexisting	This command was preexisting.

Usage Guidelines

The **ssh** *ip_address* command specifies hosts or networks that are authorized to initiate an SSH connection to the security appliance. 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 security appliance, you must generate a default RSA key using the **crypto key generate rsa** command.

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

- 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 security appliance:

- 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 security appliance.
ssh version	Restricts the security appliance 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
Preexisting	This command was preexisting.

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 security appliance.
ssh timeout	Sets the timeout value for idle SSH sessions.

ssh scopy enable

To enable Secure Copy (SCP) on the security appliance, 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
7.0(1)	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 security appliance has the following restrictions:

- There is no directory support in this implementation of SCP, limiting remote client access to the security appliance internal files.
- There is no banner support when using SCP.
- SCP does not support wildcards.
- The security appliance 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 security appliance from the specified client or network.
ssh version	Restricts the security appliance 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
Preexisting	This command was preexisting.

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 security appliance.
ssh disconnect	Disconnects an active SSH session.

ssh version

To restrict the version of SSH accepted by the security appliance, use the **ssh version** command in global configuration mode. To restore the default value, use the **no** form of this command. The default values permits SSH Version 1 and SSH Version 2 connections to the security appliance.

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
7.0(1)	This command was introduced.

Usage Guidelines

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

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 security appliance from the specified client or network.

ssl client-version

To specify the SSL/TLS protocol version the security appliance uses when acting as a client, use the **ssl client-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/TLS that the security appliance sends.

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

no ssl client-version

Syntax Description

any	The security appliance sends SSL version3 hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3-only	The security appliance sends SSL version 3 hellos, and accepts only SSL version 3.
tlsv1-only	The security appliance sends TLSv1 client hellos, and accepts 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
7.0(1)(1)	This command was introduced.

Usage Guidelines

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

Negotiate SSLv3	Java downloads
Negotiate SSLv3/TLSv1	Java downloads
Negotiate TLSv1	Java does NOT download
TLSv1Only	Java does NOT download
SSLv3Only	Java does NOT download

The issue is that JAVA only negotiates SSLv3 in the client Hello packet when you launch the Port Forwarding application.

Examples

The following example shows how to configure the security appliance to communicate using only TLSv1 when acting as an SSL client:

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

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
show running-config ssl	Displays the current set of configured SSL commands.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl encryption

To specify the encryption algorithms that the SSL/TLS protocol uses, use the **ssl encryption** command in global configuration mode**.** Issuing the command again overwrites the previous setting. The ordering of the algorithms determines preference for their use. You can add or remove algorithms to meet the needs of your environment. To restore the default, which is the complete set of encryption algorithms, use the **no** version of the command.

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*aes128-sha1*] [*aes256-sha1*] [*possibly others*]

no ssl encryption

Syntax Description

3des-sha1	Specifies triple DES encryption with Secure Hash Algorithm 1.
des-sha1	Specifies DES encryption with Secure Hash Algorithm 1.
rc4-md5	Specifies RC4 encryption with an MD5 hash function.
aes128-sha1	Specifies triple AES 128-bit encryption with Secure Hash Algorithm 1.
aes256-sha1	Specifies triple AES 256-bit encryption with Secure Hash Algorithm 1.
possibly others	Indicates that more encryption algorithms may be added in future releases.

Defaults

The default is to have all algorithms available in the following order:

[*3des-sha1***] [***des-sha1***] [***rc4-md5***] [***possibly others***]**

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
7.0(1)(1)	This command was introduced.

Usage Guidelines

The ASDM License tab reflects the maximum encryption the license supports, not the value you configure.

Examples

The following example shows how to configure the security appliance to use the 3des-sha1 and des-sha1 encryption algorithms:

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

Related Commands

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl server-version

To specify the SSL/TLS protocol version the security appliance 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 the security appliance accepts.

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

no ssl server-version

Syntax Description

any	The security appliance accepts SSL version 2 client hellos, and negotiates either SSL version 3 or TLS version 1.
sslv3	The security appliance accepts SSL version 2 client hellos, and negotiates to SSL version 3.
sslv3-only	The security appliance accepts only SSL version 3 client hellos, and uses only SSL version 3.
tlsv1	The security appliance accepts SSL version 2 client hellos, and negotiates to TLS version 1.
tlsv1-only	The security appliance 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
7.0(1)(1)	This command was introduced.

Usage Guidelines

TCP Port Forwarding does not work when a WebVPN user connects with some SSL versions, as follows:

Negotiate SSLv3	Java downloads
Negotiate SSLv3/TLSv1	Java downloads
Negotiate TLSv1	Java does NOT download
TLSv1Only	Java does NOT download
SSLv3Only	Java does NOT download

If you configure e-mail proxy, do not set thhe SSL version to TLSv1 Only. Outlook and Outlook Express do not support TLS.

Examples

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

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

Related Commands

Command	Description
clear config ssl	Removes all ssl commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured ssl commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl trust-point	Specifies the certificate trust point that represents the SSL certificate for an interface.

ssl trust-point

To specify the certificate trustpoint that represents the SSL certificate for an interface, use the **ssl trust-point** command with the *interface* argument in global configuration mode. If you do not specify an interface, this command creates the fallback trustpoint for all interfaces that do not have a trustpoint configured. To remove an SSL trustpoint from the configuration that does not specify an interface, use the **no** version of this command. To remove an entry that does specify an interface, use the **no ssl trust-point** {*trustpoint [interface]*} version of the command.

ssl trust-point {*trustpoint [interface]*}

no ssl trust-point

Syntax Description

interface	The name for the interface to which the trustpoint applies. The **nameif** command specifies the name of the interface.
trustpoint	The *name* of the CA trustpoint as configured in the **crypto ca trustpoint** {*name*} command.

Defaults

The default is no trustpoint association. The security appliance uses the default self-generated RSA key-pair certificate.

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
7.0(1)(1)	This command was introduced.

Usage Guidelines

Observe these guidelines when using this command:

- The value for *trustpoint* must be the name of the CA trustpoint as configured in the **crypto ca trustpoint {*name*}** command.
- The value for *interface* must be the *nameif* name of a previously configured interface.
- Removing a trustpoint also removes any **ssl trust-point** entries that reference that trustpoint.
- You can have one **ssl trustpoint** entry for each interface and one that specifies no interfaces.
- You can reuse the same trustpoint for multiple entries.

The following example explains how to use the **no** versions of this command:

The configuration includes these SSL trustpoints:

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

Issue the command:

no ssl trust-point

Then show run ssl will have:

ssl trust-point tp2 outside

Examples

The following example shows how to configure an ssl trustpoint called FirstTrust for the inside interface, and a trustpoint called DefaultTrust with no associated interface.

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

The next example shows how to use the **no** version of the command to delete a trustpoint that has no associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

The next example shows how to delete a trustpoint that does have an associated interface:

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

Command	Description
clear config ssl	Removes all SSL commands from the configuration, reverting to the default values.
show running-config ssl	Displays the current set of configured SSL commands.
ssl client-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a client.
ssl encryption	Specifies the encryption algorithms that the SSL/TLS protocol uses.
ssl server-version	Specifies the SSL/TLS protocol version the security appliance uses when acting as a server.

sso-server

To create a single sign-on server for security appliance user authentication, use the **sso-server** command in webvpn configuration mode. This is an SSO with CA SiteMinder command.

To remove an SSO server, use the **no** form of this command.

sso-server *name* **type** *siteminder*

no sso-server *name* **type** *siteminder*

Note This command is required for SSO authentication.

Syntax Description

name	Specifies the name of the SSO server. Minimum of 4 characters and maximum of 31 characters.
siteminder	The security appliance is compatible with CA SiteMinder so *siteminder* is only argument available.
type	Specifies the type of SSO server. SiteMinder is the only type available.

Defaults

There is no default value or behavior.

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
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once. The **sso-server** command lets you create an SSO server. Once you have created the SSO server, then, in any order, you must configure the authentication URL (see the **web-agent-url** command) and the secret key for securing communications with the server (see the **policy-server-secret** command).

In the authentication, the security appliance acts as a proxy for the WebVPN user to the SSO server. The security appliance currently supports the Computer Associates eTrust SiteMinder SSO server (formerly Netegrity SiteMinder). Thus, the available argument for the type option is *siteminder*.

Examples

The following example, entered in webvpn configuration mode, creates an SSO server named "example":

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to an SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for an SSO server.
test sso-server	Tests an SSO server with a trial authentication request.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SSO authentication requests.

sso-server value (config-group-webvpn)

To assign an SSO server to a group policy, use the **sso-server value** command in group-policy-webvpn configuration mode. This is an SSO with CA SiteMinder command.

To remove the assignment and use the default policy, use the **no** form of this command.

To prevent inheriting the default policy, use the **sso-server none** command.

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

Syntax Description

name	Specifies the name of the SSO server being assigned to the group policy.

Defaults

The default policy assigned to the group is DfltGrpPolicy.

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 webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once. The **sso-server value** command, when entered in group-policy-webvpn mode, lets you assign an SSO server to a group policy.

Note Enter the same command, **sso-server value**, in username-webvpn configuration mode to assign SSO servers to user policies.

Examples

The following example commands create the group policy my-sso-grp-pol and assigns it to the SSO server named example:

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to an SSO server.
show webvpn sso-server	Displays the operating statistics for an SSO server.
sso-server	Creates a single sign-on server.
sso-server value (config-username-webvpn)	Assigns an SSO server to a user policy.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SSO authentication requests.

sso-server value (config-username-webvpn)

To assign an SSO server to a user policy, use the **sso-server value** command in username-webvpn configuration mode. This is an SSO with CA SiteMinder command.

To remove an SSO server assignment for a user, use the **no** form of this command.

When a user policy inherits an unwanted SSO server assignment from a group policy, use the **sso-server none** command to remove the assignment.

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

Syntax Description

name	Specifies the name of the SSO server being assigned to the user policy.

Defaults

The default is for the user policy to use the SSO server assignment in the group policy.

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
Username webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once. The **sso-server value** command lets you assign an SSO server to a user policy.

Note Enter the same command, **sso-server value**, in group-webvpn configuration mode to assign SSO servers to group policies.

Examples

The following example commands assign the SSO server named my-sso-server to the user policy for a WebVPN user named Anyuser:

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value my-sso-server
hostname(config-username-webvpn)#
```

Related Commands

Command	Description
policy-server-secret	Creates a secret key used to encrypt authentication requests to an SSO server.
show webvpn sso-server	Displays the operating statistics for an SSO server.
sso-server	Creates a single sign-on server.
sso-server value (config-group-webvpn)	Assigns an SSO server to a group policy.
web-agent-url	Specifies the SSO server URL to which the security appliance makes SSO authentication requests.

start-url

To enter the URL at which to retrieve an optional pre-login cookie, use the **start-url** command in aaa-server- host configuration mode. This is an SSO with HTTP Forms command.

start-url *string*

Note To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The URL for an SSO server. The maximum URL length is 1024 characters.

Defaults

There is no default value or behavior.

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
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The WebVPN server of the security appliance can use an HTTP POST request to submit a single sign-on authentication request to an authenticating web server. The authenticating web server may execute a pre-login sequence by sending a Set-Cookie header along with the login page content. You can discover this by connecting directly to the authenticating web server's login page with your browser. If the web server sets a cookie when the login page loads and if this cookie is relevant for the following login session, you must use the **start-url** command to enter the URL at which the cookie is retrieved. The actual login sequence starts after the pre-login cookie sequence with the form submission to the authenticating web server.

Note The **start-url** command is only required in the presence of the pre-login cookie exchange.

Examples

The following example, entered in aaa-server-host configuration mode, specifies a URL for retrieving the pre-login cookie of https://example.com/east/Area.do?Page-Grp1:

```
hostname(config)# aaa-server testgrp1 (inside) host example.com
hostname(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
```

```
hostname(config-aaa-server-host)#
```

Related Commands

Command	Description
action-uri	Specifies a web server URI to receive a username and password for single sign-on authentication.
auth-cookie-name	Specifies a name for the authentication cookie.
hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
user-parameter	Specifies the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication.

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:

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

Command History

Release	Modification
7.2(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 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.

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* {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name* | **interface**} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

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

For static PAT:

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

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

Syntax Description

access-list *access_list_name*	Lets you identify real addresses for NAT by specifying the real and destination addresses (or ports). This feature is known as policy NAT. The subnet mask used in the access list is also used for the *mapped_ip*. You can only include **permit** statements in the access list. You can also specify the real and destination ports in the access list using the **eq** operator. Policy NAT does not consider the **inactive** or **time-range** keywords; all ACEs are considered to be active for policy NAT configuration.
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. **Note** DNS inspection must be enabled to support this functionality. Additionally, DNS Rewrite is not applicable for PAT because multiple PAT rules are applicable for each A-record and the PAT rule to use is ambiguous.
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 security appliance 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. Use this keyword if you want to use the interface address, but the address is dynamically assigned using DHCP. **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
nailed	(Optional) Allows TCP sessions for asymmetrically routed traffic. This option allows inbound traffic to traverse the security appliance without a corresponding outbound connection to establish the state. This command is used in conjunction with the **failover timeout** command. The **failover timeout** command specifies the amount of time after a system boots or becomes active that the nailed sessions are accepted. If not configured, the connections cannot be reestablished. **Note** Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection. Using the **asr-group** command to configure asymmetric routing support is more secure than using the **static** command with the **nailed** option and is the recommended method for configuring asymmetric routing support.
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. 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 both the inbound and outbound 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. TCP initial sequence number randomization can be disabled if required. For example: • If another in-line firewall is also randomizing the initial sequence numbers, there is no need for both firewalls to be performing this action, even though this action does not affect the traffic. • If you use eBGP multi-hop through the security appliance, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum. • You use a WAAS device that requires the security appliance not to randomize the sequence numbers of connections.
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*	Specifies the maximum number of simultaneous TCP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.)
udp	For static PAT, specifies the protocol as UDP.
udp *udp_max_conns*	(Optional) Specifies the maximum number of simultaneous UDP connections for the entire subnet. The default is 0, which means unlimited connections. (Idle connections are closed after the idle timeout specified by the **timeout conn** command.)

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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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.

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 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 mapped address for multiple static NAT statements).

You cannot use the same real or mapped address in multiple **static** commands between the same two interfaces. 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, etc.), the security appliance automatically translates the secondary ports.

NAT, in the conventional sense, is not available in transparent firewall mode. In transparent firewall mode, you can use the **static** command to configure maximum connections, maximum embryonic connections, and TCP sequence randomization. In this case, both the real and mapped IP addresses are the same.

If you specify a network for translation (for example, 10.1.1.0 255.255.255.0), then the security appliance 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.

After changing or removing a static command statement, use the **clear xlate** command to clear the translations.

You can alternatively configure maximum connections, maximum embryonic connections, and TCP sequence randomization using the **set connection** commands. If you configure these settings for the same traffic using both methods, then the security appliance uses the lower limit. For TCP sequence randomization, if it is disabled using either method, then the security appliance disables TCP sequence randomization.

The connection attributes (**dns**, **norandomseq**, **nailed**, **tcp**, and **udp**) have a per-host limit. In some cases, such as policy NAT (with an access list) or NAT involving more than two interfaces, a connection attribute can derive its value from multiple **nat** and **static** commands. In such cases, the value from the rule that matches the first packet is the value that takes precedent. For example, with the following configuration, TCP connection limits of 100 and 200 can be applicable:

```
static (inside,dmz) 192.168.1.1 192.168.1.100 tcp 100
static (inside,outside) 192.168.1.1 192.168.1.100 tcp 200
```

If the first packet from host 192.168.1.1 is toward the dmz interface, the TCP connection limit is 100 for all subsequent TCP sessions.

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
```

This example shows how to permit a finite number of users to call in through H.323 using Intel Internet Phone, CU-SeeMe, CU-SeeMe Pro, MeetingPoint, or Microsoft NetMeeting. The **static** command maps addresses 209.165.201.0 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
```

This 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 security appliance 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 eq telnet 10.1.3.0
255.255.255.0
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 security appliance 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 eq http 10.1.3.0
255.255.255.0
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

To redirect Telnet traffic from the security appliance 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.
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 of a violation occurs.
log	Specifies standalone or additional log in case of violation. 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
7.2(1)	This command was introduced.

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.

Command	Description
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
7.0(1)	This command was introduced.

Usage Guidelines

Although strict HTTP inspection cannot be disabled, the **strict-http action allow** command causes the security appliance 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
hostname(config-http-map)#
```

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 security appliance selects the tunnel group for IPSec connections by obtaining the group name from the username presented by the VPN client. When strip-group processing is enabled, the security appliance sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the security appliance 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
7.0.1	This command was introduced.

Usage Guidelines

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

Note Because of a limitation of MSCHAPv2, you cannot perform tunnel group switching when MSCHAPv2 is used for PPP authentication. The hash computation during MSCHAPv2 is bound to the username string (such as user + delimt + group).

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-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-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 general-attributes	Specifies the general attributes for the named tunnel-group.

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 security appliance sends only the user part of the username authorization/authentication. Otherwise, the security appliance 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
7.0.1	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-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-realm
```

neral)

ostname(config-ge

Related Commands

h

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups or the specified tunnel-group.
show running-config tunnel-group	Shows the current tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.

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 an 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*	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
7.0(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
```

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
7.0(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//:frog.phoobin.com and includes the subject DN OU tiedye.com in the the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=tiedye.com
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

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
Preexisting	This command was preexisting.

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.
port- *port*	(Optional) Specifies the SunRPC protocol port range.
protocol tcp	Specifies the SunRPC transport protocol.
protocol udp	Specifies the SunRPC transport protocol.
service	Specifies a service.
service_type	Sets the SunRPC service program number as specified in the **sunrpcinfo** 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
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to create an SunRPC services table:

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

Related Commands

Command	Description
clear configure sunrpc-server	Clears the Sun remote processor call services from the security appliance.
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
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance 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.

svc

To enable or require the SVC for a specific group or user, use the **svc** command in the group-policy and username webvpn modes.

To remove the **svc** command from the configuration, use the **no** form of the command:

svc {**none** | **enable** | **required**}

no svc

To remove the command from the configuration and cause the value to be inherited, use the **no** form of the command.

Syntax Description

none	Disables the SVC for this group or user.
enable	Enables the SVC for this group or user.
required	SVC is required for this group or user.

Defaults

The default is **none**. SVC is disabled in the group policy or user policy.

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 webvpn	•	—	•	—	—
username webvpn	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Examples

In the following example, the user configures the existing group-policy *sales* to require the SVC:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc required
```

Related Commands

Command	Description
show webvpn svc	Displays information about the SVC installation.

svc enable	Enables the security appliance to download SVC files to remote computers.
svc image	Causes the security appliance to load SVC files from flash memory to RAM, and specifies the order in which the security appliance downloads SVC files to the remote computer.

svc compression

To enable compression of http data over an SVC connection for a specific group or user, use the **svc compression** command in the group policy and username webvpn modes.

To remove the **svc compression** command from the configuration and cause the value to be inherited, use the **no** form of the command:

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

Syntax Description

deflate	Specifies compression is enabled for the group or user.
none	Specifies compression is disabled for the group or user.

Defaults

By default, SVC compression is set to *deflate* (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
group-policy webvpn	•	—	•	—	—
username webvpn	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

For SVC connections, the **compression** command configured from global configuration mode overrides the **svc compression** command configured in group policy and username webvpn modes.

Examples

In the following example, SVC compression is disabled for the group-policy sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

Related Commands

Command	Description
compression	Enables compression for all SVC, WebVPN, and IPSec VPN connections.
show webvpn svc	Displays information about the SVC installation.

svc dpd-interval

To enable DPD on the security appliance and to set the frequency that either the SVC or the security appliance performs DPD, use the **svc dpd-interval** command from group policy or username webvpn mode:

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited.

Syntax Description

gateway *seconds*	Specifies the frequency, from 30 to 3600 seconds, that the security appliance performs DPD.
gateway none	Disables DPD that the security appliance performs.
client *seconds*	Specifies the frequency, from 30 to 3600 seconds, that the SVC performs DPD.
client none	Disables DPD that the SVC performs.

Defaults

The default is none. DPD is disabled for both the SVC and the security appliance.

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
WebVPN Group Policy	•	—	•	—	—
WebVPN Username	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

In the following example, the user configures the DPD frequency performed by the security appliance (gateway) to 3000 seconds, and the DPD frequency performed by the client to 1000 seconds, for the existing group policy named Sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
```

Related Commands

Command	Description
svc	Enables or requires the SVC for a specific group or user.

svc keepalive	Specifies the frequency at which an SVC on a remote computer sends keepalive messages to the security appliance.
svc keep-installer	Enables the permanent installation of an SVC onto a remote computer.
svc rekey	Enables the SVC to perform a rekey on an SVC session.

svc enable

To enable the security appliance to download SVC files to remote computers, use the **svc enable** command from webvpn mode.

To remove the **svc enable** command from the configuration, use the **no** form of this command:

svc enable

no svc enable

Defaults

The default for this command is disabled. The security appliance does not download SVC files.

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
webvpn	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

Entering the **no svc enable** command does not terminate active SVC sessions.

Examples

In the following example, the user enables the security appliance to download SVC files:

```
(config)# webvpn
(config-webvpn)# svc enable
```

Related Commands

Command	Description
show webvpn svc	Displays information about the SVC installation.
svc	Enables or requires the SVC for a specific group or user.
svc image	Causes the security appliance to load SVC files from flash memory into RAM, and specifies the order in which the security appliance downloads SVC files to the remote computer.

svc image

To cause the security appliance to load SVC files from flash memory into RAM, and to specify the order in which the security appliance downloads SVC files to the remote computer, use the **svc image** command from webvpn mode.

To remove the **svc image** command from the configuration, use the **no** form of the command:

svc image *filename order*

no svc image *filename order*

Syntax Description

filename	Specifies the filename of the SVC file, up to 255 characters.
order	Specifies a number indicating the relative position of the files to each other, from 1 to 65535.

Defaults

The default order 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
webvpn mode	•	—	•	—	—

Command History

Release	Modification
7.1.1	This command was introduced.

Usage Guidelines

Numbering of the SVC files establishes the order in which the security appliance downloads them to the remote computer. It downloads the SVC file with the lowest number first. Therefore, you should assign the lowest number to the file that the most commonly-encountered operating system uses.

You can configure the files in any order. For example, you can configure 2 before 1.

Examples

In the following example, the output of the **show webvpn svc** command indicates that the windows.pkg file has an order number of 1, and the windows2.pkg file has an order number of 15. When a remote computer attempts to establish an SVC connection, the windows.pkg file downloads first. If the file does not match the operating system, the windows2.pkg file downloads:

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43
```

```
2. disk0:/windows2.pkg 15
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

The user then reorders the SVC archive files using the **svc image** command, with the windows2.pkg file as the first file downloaded to the remote PC, and the windows.pkg file downloaded second:

```
hostname(config-webvpn)# svc image windows2.pkg 10
hostname(config-webvpn)# svc image windows.pkg 20
```

Reentering the **show webvpn svc** command shows the new order of the files.

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 10
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 20
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

Related Commands

Command	Description
show webvpn svc	Displays information about the SVC installation.
svc	Enables or requires the SVC for a specific group or user.
svc enable	Enables the security appliance to download the SVC files to remote computers.

svc keepalive

To configure the frequency which an SVC on a remote computer sends keepalive messages to the security appliance, use the **svc keepalive** command.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

svc keepalive {**none** | *seconds*}

no svc keepalive {**none** | *seconds*}

Syntax Description

none	Disables SVC keepalive messages.
seconds	Enables the SVC to send keepalive messages, and specifies the frequency of the messages in a range of 15 to 600 seconds.

Defaults

The default is none (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**
WebVPN Group Policy	•	—	•	—	—
WebVPN Username	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

You can adjust the frequency of keepalive messages (specified by *seconds*), to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.

Adjusting the frequency also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

Examples

In the following example, the user configures the security appliance to enable the SVC to send keepalive messages, with a frequency of 300 seconds (5 minutes), for the existing group policy named Sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

Related Commands

Command	Description
svc	Enables or requires the SVC for a specific group or user.
svc dpd-interval	Enables Dead Peer Detection (DPD) on the security appliance, and sets the frequency that either the SVC or the security appliance performs DPD.
svc keep-installer	Enables the permanent installation of an SVC onto a remote computer.
svc rekey	Enables the SVC to perform a rekey on an SVC session.

svc keep-installer

To enable the permanent installation of an SVC onto a remote computer, use the **svc keep-installer** command from group-policy or username webvpn modes.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

Syntax Description

installed	Specifies that the SVC is installed permanently on the remote computer.
none	Specifies that the SVC uninstalls from the remote computer after the active SVC connection terminates.

Defaults

The default is permanent installation of the SVC is disabled. The SVC uninstalls from the remote computer at the end of the SVC session.

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**
WebVPN Group Policy	•	—	•	—	—
WebVPN Username	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Examples

In the following example, the user configures the group policy to keep the SVC installed on the remote computer:

```
hostname(config-group-policy)# svc keep-installer installed
hostname(config-group-policy)#
```

Related Commands

Command	Description
show webvpn svc	Displays information about the SVC installation.
svc	Enables or requires the SVC for a specific group or user.

svc enable	Causes the security appliance to download SVC files from flash memory to RAM.
svc image	Specifies the order in which the security appliance downloads SVC files to the remote computer.

svc rekey

To enable the SVC to perform a rekey on an SVC session, use the **svc rekey** command from group-policy and username webvpn modes.

Use the **no** form of the command to remove the command from the configuration and cause the value to be inherited:

svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

Syntax Description

method ssl	Specifies that SSL renegotiation takes place during SVC rekey.
method new-tunnel	Specifies that the SVC establishes a new tunnel during SVC rekey.
time *minutes*	Specifies the number of minutes from the start of the session until the re-key takes place, from 4 to 10080 (1 week).
method none	Disables SVC rekey.

Defaults

The default is none (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
WebVPN Group Policy	•	—	•	—	—
WebVPN Username	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

We recommend that you configure SSL as the rekey method.

Examples

In the following example, the user configures the SVC to renegotiate with SSL during rekey and configures the rekey to occur 30 minutes after the session begins, for the existing group policy named Sales:

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc rekey method ssl
hostname(config-group-webvpn)# svc rekey time 30
```

Related Commands

Command	Description
svc	Enables or requires the SVC for a specific group or user.
svc dpd-interval	Enables Dead Peer Detection (DPD) on the security appliance, and sets the frequency that either the SVC or the security appliance performs DPD.
svc keepalive	Specifies the frequency at which an SVC on a remote computer sends keepalive messages to the security appliance.
svc keep-installer	Enables the permanent installation of an SVC onto a remote computer.

switchport access vlan

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport access vlan** command in interface configuration mode to assign a switch port to a VLAN.

switchport access vlan *number*

no switchport access vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID to which you want to assign this switch port. The VLAN ID is between 1 and 1001.

Defaults

By default, all switch ports are assigned to VLAN 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
Interface configuration	•	•	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

In transparent firewall mode, you can configure two active VLANs in the ASA 5505 adaptive security appliance Base license and three active VLANs in the Security Plus license, one of which must be for failover.

In routed mode, you can configure up to three active VLANs in the ASA 5505 adaptive security appliance Base license, and up to 20 active VLANs with the Security Plus license.

An active VLAN is a VLAN with a **nameif** command configured.

You can assign one or more physical interfaces to each VLAN using the **switchport access vlan** command. By default, the VLAN mode of the interface is to be an access port (one VLAN associated with the interface). If you want to create a trunk port to pass multiple VLANs on the interface, use the **switchport mode access trunk** command to change the mode to trunk mode, and then use the **switchport trunk allowed vlan** command.

Examples

The following example assigns five physical interfaces to three VLAN interfaces:

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown
```

```
hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport protected	Prevents a switch port from communicating with other switch ports on the same VLAN for extra security.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport mode

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport mode** command in interface configuration mode to set the VLAN mode to either access (the default) or trunk.

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

Syntax Description

access	Sets the switch port to access mode, which allows the switch port to pass traffic for only one VLAN. Packets exit the switch port without an 802.1Q VLAN tag. If a packet enters the switch port with a tag, the packet is dropped.
trunk	Sets the switch port to trunk mode, so it can pass traffic for multiple VLANs. Packets exit the switch port with an 802.1Q VLAN tag. If a packet enters the switch port without a tag, the packet is dropped.

Defaults

By default, the mode is access.

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
7.2(1)	This command was introduced.
7.2(2)	You can now configure multiple trunk ports, rather than being limited to one trunk.

Usage Guidelines

By default, the VLAN mode of the switch port is to be an access port (one VLAN associated with the switch port). In access mode, assign a switch port to a VLAN using the **switchport access vlan** command. If you want to create a trunk port to pass multiple VLANs on the switch port, set the mode to trunk mode, and then use the **switchport trunk allowed vlan** command to assign multiple VLANs to the trunk. If you set the mode to trunk mode, and you have not yet configured the **switchport trunk allowed vlan** command, the switch port remains in "line protocol down" state and cannot participate in traffic forwarding. Trunk mode is available only with the Security Plus license.

The **switchport vlan access** command does not take effect unless the mode is set to access mode. The **switchport trunk allowed vlan** command does not take effect unless the mode is set to trunk mode.

Examples

The following example configures an access mode switch port assigned to VLAN 100, and a trunk mode switch port assigned to VLANs 200 and 300:

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200,300
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport protected	Prevents a switch port from communicating with other switch port on the same VLAN for extra security.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport monitor

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport monitor** command in interface configuration mode to enable SPAN, also known as switch port monitoring. The port for which you enter this command (called the destination port) receives a copy of every packet transmitted or received on the specified source port. The SPAN feature lets you attach a sniffer to the destination port so you can monitor traffic. You can specify multiple source ports by entering this command multiple times. You can only enable SPAN for one destination port. To disable monitoring of a source port, use the **no** form of this command.

switchport monitor *source_port* [**tx** | **rx** | **both**]

no switchport monitor *source_port* [**tx** | **rx** | **both**]

Syntax Description

source_port	Specifies the port you want to monitor. You can specify any Ethernet port as well as the Internal-Data0/1 backplane port that passes traffic between VLAN interfaces. Because the Internal-Data0/1 port is a Gigabit Ethernet port, you might overload the Fast Ethernet destination port with traffic. Monitor the port Internal-Data0/1 with caution.
tx	(Optional) Specifies that only transmitted traffic is monitored.
rx	(Optional) Specifies that only received traffic is monitored.
both	(Optional) Specifies that both transmitted and received traffic is monitored. **both** is the default.

Defaults

The default type of traffic to monitor is **both**.

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
7.2(1)	This command was introduced.

Usage Guidelines

If you do not enable SPAN, then attaching a sniffer to one of the switch ports only captures traffic to or from that port. To capture traffic to or from multiple ports, you need to enable SPAN and identify the ports you want to monitor.

Use caution while connecting a SPAN destination port to another switch, as it could result in network loops.

Examples

The following example configures the Ethernet 0/1 port as the destination port which monitors the Ethernet 0/0 and Ethernet 0/2 ports:

```
hostname(config)# interface ethernet 0/1
hostname(config-if)# switchport monitor ethernet 0/0
hostname(config-if)# switchport monitor ethernet 0/2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport protected	Prevents a switch port from communicating with other switch port on the same VLAN for extra security.

switchport protected

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport protected** command in interface configuration mode to prevent the switch port from communicating with other protected switch ports on the same VLAN. This feature provides extra security to the other switch ports on a VLAN if one switch port becomes compromised.

switchport protected

no switchport protected

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the interfaces are not protected.

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
7.2(1)	This command was introduced.

Usage Guidelines

You might want to prevent switch ports from communicating with each other if the devices on those switch ports are primarily accessed from other VLANs, you do not need to allow intra-VLAN access, and you want to isolate the devices from each other in case of infection or other security breach. For example, if you have a DMZ that hosts three web servers, you can isolate the web servers from each other if you apply the **switchport protected** command to each switch port. The inside and outside networks can both communicate with all three web servers, and vice versa, but the web servers cannot communicate with each other.

Communication to and from unprotected ports is not restricted by this command.

Examples

The following example configures seven switch ports. The Ethernet 0/4, 0/5, and 0/6 are assigned to the DMZ network and are protected from each other.

```
hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
```

```
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/5
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/6
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.
switchport access vlan	Assigns the switch port to a VLAN.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport trunk allowed vlan	Assigns VLANs to a trunk port.

switchport trunk

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **switchport trunk** command in interface configuration mode to assign VLANs to the trunk port. To remove one or more VLANs from the trunk, use the **no** form of this command.

switchport trunk {**allowed vlan** *vlan_range* | **native vlan** *vlan_id*}

no switchport trunk {**allowed vlan** *vlan_range* | **native vlan** *vlan_id*}

Syntax Description

allowed	Specifies tagged VLANs.
native	Specifies native VLANs. Packets on the native VLAN are not modified when sent over the trunk. For example, if a port has VLANs 2, 3 and 4 assigned to it, and VLAN 2 is the native VLAN, then packets on VLAN 2 that egress the port are not modified with an 802.1Q header. Frames which ingress (enter) this port and have no 802.1Q header are put into VLAN 2. Each port can only have one native VLAN, but every port can have either the same or a different native VLAN.
vlan *vlan_id*	Identifies the native VLAN for this port, between 1 and 4090.
vlan *vlan_range*	Identifies one or more VLANs that you can assign to the trunk port. The VLAN ID is between 1 and 4090. The *vlan_range* can be identified in one of the following ways: • A single number (n) • A range (n-x) Separate numbers and ranges by commas, for example: 5,7-10,13,45-100 You can enter spaces instead of commas, but the command is saved to the configuration with commas. You can include the native VLAN in this value, but it is not required; the native VLAN is passed whether it is included in this value or not.

Defaults

By default, no VLANs are assigned to the trunk.

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
7.2(1)	This command was introduced.
7.2(2)	This command was modified to allow more than 3 VLANs per switch port. Also, you can now configure multiple trunk ports, instead of being limited to only one. This command also uses commas instead of spaces to separate VLAN IDs.
7.2(4)	The **native** keyword was added.

Usage Guidelines

If you want to create a trunk port to pass multiple VLANs on the switch port, set the mode to trunk mode, and then use the **switchport trunk** command to assign multiple VLANs to the trunk. This switch port cannot pass traffic until you assign at least one VLAN to it, either native or non-native. If you set the mode to trunk mode, and you have not yet configured the **switchport trunk** command, the switch port remains in "line protocol down" state and cannot participate in traffic forwarding. Trunk mode is available only with the Security Plus license.

The **switchport trunk** command does not take effect unless the mode is set to trunk mode.

If you use the **no switchport trunk** command, you can remove all VLANs or a subset of VLANs from the trunk.

Note This command is not downgrade-compatible to Version 7.2(1); the commas separating the VLANs are not recognized in 7.2(1). If you downgrade, be sure to separate the VLANs with spaces, and do not exceed the 3 VLAN limit.

Examples

The following example configures an access mode switch port assigned to VLAN 100, a trunk mode switch port assigned to VLANs 200, 201, and 202 and native VLAN 50, and another trunk mode switch port assigned to VLANs 300, 301, and 305:

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 50
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 300,301,305
hostname(config-if)# no shutdown

...
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the interface configuration in the running configuration.

Command	Description
switchport access vlan	Assigns the switch port to a VLAN.
switchport mode	Sets the VLAN mode to be access or trunk.
switchport protected	Prevents a switch port from communicating with other switch ports on the same VLAN for extra security.

synack-data

To set the action for TCP SYNACK packets that contain data, use the **synack-data** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

synack-data {**allow** | **drop**}

no synack-data

Syntax Description

allow	Allows TCP SYNACK packets that contain data.
drop	Drops TCP SYNACK packets that contain data.

Defaults

The default action is to drop TCP SYNACK packets that contain data.

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
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.2(4)	This command was introduced.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **synack-data**—In tcp-map configuration mode, you can enter the **synack-data** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example sets the security appliance to allow TCP SYNACK packets that contain data:

```
hostname(config)# tcp-map tmap
```

```
hostname(config-tcp-map)# synack-data allow
hostname(config)# class-map cmap
hostname(config-cmap)# match any
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class-map	Identifies traffic for a service policy.
policy-map	dentifies actions to apply to traffic in a service policy.
set connection advanced-options	Enables TCP normalization.
service-policy	Applies a service policy to interface(s).
show running-config tcp-map	Shows the TCP map configuration.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

syn-data

To allow or drop SYN packets with data, use the **syn-data** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

Syntax Description

allow	Allows SYN packets that contain data.
drop	Drops SYN packets that contain data.

Defaults

Packets with SYN data are allowed 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
Tcp-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **syn-data**—In tcp-map configuration mode, you can enter the **syn-data** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the tcp-map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

According to the TCP specification, TCP implementations are required to accept data contained in a SYN packet. Because this is a subtle and obscure point, some implementations may not handle this correctly. To avoid any vulnerabilities to insertion attacks involving incorrect end-system implementations, you may choose to drop packets with data in SYN packets.

Examples

The following example shows how to drop SYN packets with data on all TCP flows:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# syn-data drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

sysopt connection permit-vpn

For traffic that enters the security appliance through a VPN tunnel and is then decrypted, use the **sysopt connection permit-vpn** command in global configuration mode to allow the traffic to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic. To disable this feature, use the **no** form of this command.

sysopt connection permit-vpn

no sysopt connection permit-vpn

Syntax Description

This command has no arguments or keywords.

Defaults

This feature 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
7.0(1)(1)	This command is now enabled by default. Also, only interface access lists are bypassed; group policy or per-user access lists remain in force.
7.1(1)	This command was changed from **sysopt connection permit-ipsec**.

Usage Guidelines

By default, the security appliance allows VPN traffic to terminate on a security appliance interface; you do not need to allow IKE or ESP (or other types of VPN packets) in an interface access list. By default, you also do not need an interface access list for local IP addresses of decrypted VPN packets. Because the VPN tunnel was terminated successfully using VPN security mechanisms, this feature simplifies configuration and maximizes the security appliance performance without any security risks. (Group policy and per-user authorization access lists still apply to the traffic.)

You can require an interface access list to apply to the local IP addresses by entering the **no sysopt connection permit-vpn** command. See the the **access-list** and **access-group** commands to create an access list and apply it to an interface. The access list applies to the local IP address, and not to the original client IP address used before the VPN packet was decrypted.

Examples

The following example requires decrypted VPN traffic to comply with interface access lists:

```
hostname(config)# no sysopt connection permit-vpn
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

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	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
Preexisting	This command was preexisting.

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 security appliance 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 security appliance 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 security appliance alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the security appliance 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 security appliance 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 security appliance 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 permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection timewait	Forces each TCP connection to linger in a shortened TIME_WAIT state after the final normal TCP close-down sequence.

sysopt connection timewait

To force each TCP connection to linger in a shortened TIME_WAIT state of at least 15 seconds after the final normal TCP close-down sequence, use the **sysopt connection timewait** command in global configuration mode. To disable this feature, use the **no** form of this command. You might want to use this feature if an end host application default TCP terminating sequence is a simultaneous close.

An RST packet (not a normal TCP close-down sequence) will also trigger the 15 second delay. The firewall holds on to the connection for 15 seconds the last packet on conn (either FIN/ACK or RST).

sysopt connection timewait

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
Preexisting	This command was preexisting.

Usage Guidelines

The default behavior of the security appliance is to track the shutdown sequence and release the connection after two FINs and the ACK of the last FIN segment. This quick release heuristic enables the security appliance to sustain a high connection rate, based on the most common closing sequence, known as the normal close sequence. However, in a simultaneous close, both ends of the transaction initiate the closing sequence, as opposed to the normal close sequence where one end closes and the other end acknowledges prior to initiating its own closing sequence (see RFC 793). Thus, in a simultaneous close, the quick release forces one side of the connection to linger in the CLOSING state. Having many sockets in the CLOSING state can degrade the performance of an end host. For example, some WinSock mainframe clients are known to exhibit this behavior and degrade the performance of the mainframe server. Using the **sysopt connection timewait** command creates a window for the simultaneous close down sequence to complete.

Examples

The following example enables the timewait feature:

```
hostname(config)# sysopt connection timewait
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-ipsec	Permits any packets that come from an IPSec tunnel without checking any ACLs for interfaces.
sysopt connection tcpmss	Overrides the maximum TCP segment size or ensures that the maximum is not less than a specified size.

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
Preexisting	This command was preexisting.

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	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
Preexisting	This command was preexisting.

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 security appliance uses proxy ARP when you configure NAT and specify a global address that is on the same network as the security appliance interface. The only way traffic can reach the hosts is if the security appliance uses proxy ARP to claim that the security appliance 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 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
Preexisting	This command was preexisting.

Usage Guidelines

Some RADIUS servers fail to include the key in the authenticator hash within the accounting acknowledgment response. This usage caveat can cause the security appliance to continually retransmit the accounting request. Use the **sysopt radius ignore-secret** command to ignore the key in these acknowledgments, thus avoiding the retransmit problem. (The key identified here is the same one 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.