CHAPTER 63

subject-name through sysopt radius ignore-secret Commands

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 crypto 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:

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	Multiple 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 configuration 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 configurationmode.
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. Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains commas or spaces. For example: **cn=crl,ou=certs,o="cisco systems, inc.",c=US**. The maximum length is 500 characters.

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.example.com and includes the subject DN OU certs in the enrollment request for trustpoint central:

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

subject-name-default

To specify a generic subject-name distinguished name (DN) to be appended to the username in all user certificates issued by the local CA server, use the **subject-name-default** command in CA server configuration mode. To reset the subject-name DN to the default value, use the **no** form of this command.

subject-name-default *dn*

no subject-name-default

Syntax Description

dn	Specifies the generic subject-name DN included with a username in all user certificates issued by the local CA server. Supported DN attributes are cn (common name), ou (organizational unit), ol (organization locality), st (state), ea (e-mail address), c (company), t (title), and sn (surname). Use commas to separate attribute-value pairs. Insert quotation marks around any value that contains a comma. The *dn* can be up to 500 characters.

Defaults

This command is not part of the default configuration. This command specifies the default DN in the certificate. The ASA ignores this command if the user entry has a DN.

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
CA server configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **subject-name-default** command specifies a common, generic DN to be used with a username to form a subject name for issued certificates. The *dn* value cn=username is sufficient for this purpose. This command eliminates the need to define a subject-name DN specifically for each user. The DN field is optional when a user is added using the **crypto ca server user-db add** dn *dn* command.

The ASA uses this command only when issuing certificates if a user entry does not specify a DN.

Examples

The following example specifies a DN:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# subject-name-default cn=cisco,cn=example_corp,ou=eng,st=ma,
c="cisco systems, inc."
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage a local CA.
issuer-name	Specifies the subject-name DN of the certificate authority certificate.
keysize	Specifies the size of the public and private keys generated at user certificate enrollment.
lifetime	Specifies the lifetime of the CA certificate, issued certificates, or the CRL.

subnet

To configure a subnet for a network object, use the **subnet** command in object configuration mode. Use the **no** form of this command to remove the object from the configuration.

subnet {*ipv4_net_addr net_mask* | *ipv6_prefix*/*mask*}

no subnet {*ipv4_net_addr net_mask* | *ipv6_prefix*/*mask*}

Syntax Description

ipv4_net_addr	Specifies the IPv4 network address.
net_mask	Specifies the subnet mask.
ipv6_prefix/*mask*	Specifies the IPv6 prefix and mask.

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
Object network configuration	•	•	•	•	—

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

If you configure an existing network object with a different IP address, the new configuration will replace the existing configuration.

Examples

The following example shows how to create a subnet network object:

```
hostname (config)# object network OBJECT_SUBNET
hostname (config-network-object)# subnet 10.1.1.0 255.255.255.0
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.
fqdn	Specifies a fully-qualified domain name network object.
host	Specifies a host network object.

Command	Description
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.
range	Specifies a range of addresses for the network object.
show running-config object network	Shows the network object configuration.

summary-address (EIGRP)

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

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

no summary-address *as-number addr mask*

Syntax Description

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

Defaults

The defaults are as follows:

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

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

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

Examples

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

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

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

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

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

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

Related Commands

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

summary-address (OSPFv2)

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.
9.0(1)	Multiple context mode is supported.

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.

summary-prefix (OSPFv3)

To configure an IPv6 summary prefix, use the **summary-prefix** command in IPv6 router configuration mode. To restore the default, use the **no** form of this command.

summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

no summary-prefix *prefix* [**not-advertise**] [**tag** *tag_value*]

Syntax Description

not-advertise	(Optional) Suppresses routes that match the specified prefix and mask pair. This keyword applies to OSPFv3 only.
prefix	Specifies the IPv6 prefix for the destination.
tag *tag_value*	(Optional) Specifies the tag value that can be used as a match value for controlling redistribution by means of route maps. This keyword applies to OSPFv3 only.

Defaults

The defaults are as follows:

- *tag_value* is 0.
- Routes that match the specified prefix and 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
IPv6 router configuration	•	—	•	•	—

Command History

Release	Modification
9.0(1)	This command was introduced.

Usage Guidelines

Use this command to configure an IPv6 summary prefix.

Examples

In the following example, the summary prefix FECO::/24 includes addresses FECO::/1 through FECO::/24. Only the address FECO::/24 is advertised in an external LSA:

```
hostname(config-if)# ipv6 router ospf 1
hostname(config-router)# router-id 172.16.3.3
hostname(config-router)# summary-prefix FECO::/24
hostname(config-router)# redistribute static
```

Related Commands

Command	Description
ipv6 router ospf	Enters router configuration mode for OSPFv3.
redistribute	Redistributes IPv6 routes from one OSPFv3 routing domain into another OSPFv3 routing domain.

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 ASA 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 ASA.
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 ASA 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.

sw-module module password-reset

To reset the password on the software module to the default value, "cisco," use the **sw-module module password-reset** command in privileged EXEC mode.

sw-module module *id* **password-reset**

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.6(1)	This command was introduced.
9.1(1)	We added support for the ASA CX software module by adding the **cxsc** keyword.

Usage Guidelines

After resetting the password, you should change it to a unique value using the module application. Resetting the module password causes the module to reboot. Services are not available while the module is rebooting, which may take several minutes. You can run the **show module** command to monitor the module state.

The command always prompts for confirmation. If the command succeeds, no other output appears. If the command fails, an error message appears that explains why the failure occurred.

This command is only valid when the module is in the Up state.

The default password depends on the module:

- ASA IPS—The default password is **cisco** for user cisco.
- ASA CX—The default password is **Admin123** for user admin.

Examples

The following example resets a password on the IPS module:

```
hostname# sw-module module ips password-reset
Reset the password on module ips? [confirm] y
```

Related Commands

Command	Description
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module reset	Shuts down and reloads the module.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module recover

To load a recovery software image from disk for a software module, or to configure the image location, use the **sw-module module recover** command in privileged EXEC mode. You might need to recover a module using this command if, for example, the module is unable to load the current image.

sw-module module *id* **recover** {**boot** | **stop** | **configure image** *path*}

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.
boot	Initiates recovery of this module and downloads a recovery image according to the **configure** settings. The module then reboots from the new image.
configure image *path*	Configures the new image location on the local disk, for example, disk0:image2.
stop	Stops the recovery action. The module boots from the original image. You must enter this command within 30 seconds after starting recovery using the **sw-module module** *id* **recover boot** command. If you issue the **stop** command after this period, it might cause unexpected results, such as the module becoming unresponsive.

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
8.6(1)	This command was introduced.
9.1(1)	We added support for the ASA CX software module by adding the **cxsc** keyword.

Usage Guidelines

If the module suffers a failure, and the module application image cannot run, you can reinstall a new image on the module from the local disk.

This command is only available when the module is in the Up, Down, Unresponsive, or Recovery state. See the **show module** command for state information. If the module is not in an Up state, the ASA will forcefully shutdown the module. A forced shutdown will destroy the old module disk image, including any configuration, and should only be used as a disaster recovery mechanism.

You can view the recovery configuration using the **show module** *id* **recover** command.

Note Do not use the **upgrade** command within the module software to install the image.

Examples

The following example sets the module to download an image from disk0:image2:

```
hostname# sw-module module ips recover configure image disk0:image2
```

The following example recovers the module:

```
hostname# sw-module module ips recover boot
The module in slot ips will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot ips? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
sw-module module reset	Shuts down a module and performs a reset.
sw-module module reload	Reloads the module software.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module reload

To reload module software for a software module, use the **sw-module module reload** command in privileged EXEC mode.

sw-module module *id* **reload**

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.

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
8.6(1)	This command was introduced.
9.1(1)	We added support for the ASA CX software module by adding the **cxsc** keyword.

Usage Guidelines

This command differs from the **sw-module module reset** command, which also performs a reset before reloading the module.

This command is only valid when the module status is Up. See the **show module** command for state information.

Examples

The following example reloads the IPS module:

```
hostname# sw-module module ips reload
Reload module in slot ips? [confirm] y
Reload issued for module in slot ips
%XXX-5-505002: Module in slot ips is reloading.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reset	Shuts down a module and performs a reset.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module reset

To reset the module and then reload the module software, use the **sw-module module reset** command in privileged EXEC mode.

sw-module module *id* **reset**

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.

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
8.6(1)	This command was introduced.
9.1(1)	We added support for the ASA CX software module by adding the **cxsc** keyword.

Usage Guidelines

When the module is in an Up state, the **sw-module module reset** command prompts you to shut down the software before resetting.

You can recover a module using the **sw-module module recover** command. If you enter the **sw-module module reset** command while the module is in a Recover state, the module does not interrupt the recovery process. The **sw-module module reset** command performs a reset of the module, and the module recovery continues after the reset. You might want to reset the module during recovery if the module hangs; a reset might resolve the issue.

This command differs from the **sw-module module reload** command, which only reloads the software and does not perform a reset.

This command is only valid when the module status is Up, Down, Unresponsive, or Recover. See the **show module** command for state information.

Examples

The following example resets an IPS module that is in the Up state:

```
hostname# sw-module module ips reset
The module in slot ips should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot ips? [confirm] y
```

```
Reset issued for module in slot ips
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
%XXX-5-505003: Module in slot ips is resetting.  Please wait...
%XXX-5-505006: Module in slot ips is Up.
```

Related Commands

Command	Description
debug module-boot	Shows debug messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module shutdown	Shuts down the module software in preparation for being powered off without losing configuration data.
show module	Shows module information.

sw-module module shutdown

To shut down the module software, use the **sw-module module shutdown** command in privileged EXEC mode.

sw-module module *id* **shutdown**

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.

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
8.6(1)	This command was introduced.
9.1(1)	We added support for the ASA CX software module by adding the **cxsc** keyword.

Usage Guidelines

Shutting down the module software prepares the module to be safely powered off without losing configuration data.

This command is only valid when the module status is Up or Unresponsive. See the **show module** command for state information.

Examples

The following example shuts down an IPS module:

```
hostname# sw-module module ips shutdown
Shutdown module in slot ips? [confirm] y
Shutdown issued for module in slot ips
hostname#
%XXX-5-505001: Module in slot ips is shutting down.  Please wait...
%XXX-5-505004: Module in slot ips shutdown is complete.
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.
sw-module module reset	Shuts down a module and performs a reset.
show module	Shows module information.

sw-module module uninstall

To uninstall a software module image and associated configuration, use the **sw-module module uninstall** command in privileged EXEC mode.

sw-module module *id* **uninstall**

Syntax Description

id	Specifies the module ID, either **cxsc** or **ips**.

Command Default

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
8.6(1)	We introduced this command.
9.1(1)	We added support for the ASA CX software module by adding the **cxsc** keyword.

Usage Guidelines

This command permanently uninstalls the software module image and associated configuration.

Examples

The following example uninstalls the IPS module image and configuration:

```
hostname# sw-module module ips uninstall
Module ips will be uninstalled. This will completely remove the
disk image associated with the sw-module including any configuration
that existed within it.

Uninstall module <id>? [confirm]
```

Related Commands

Command	Description
debug module-boot	Shows debugging messages about the module booting process.
sw-module module recover	Recovers a module by loading a recovery image from disk.
sw-module module reload	Reloads the module software.

Command	Description
sw-module module reset	Shuts down a module and performs a reset.
show module	Shows module information.

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 4090.

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. Use the **no** form of the command to remove a VLAN from the trunk.

switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

no switchport trunk {allowed vlans *vlan_range* **| native vlan** v*lan*}

Syntax Description

allowed vlans *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 command, but it is not required; the native VLAN is passed whether it is included in this command or not.
native vlan *vlan*	Assigns a native VLAN to the trunk. 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 that 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.

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)/8.0(4)	Native VLAN support was introduced with the **native vlan** keywords.

Usage Guidelines

If you want to create a trunk port to pass multiple VLANs on the switch port, set the mode to trunk mode using the **switchport mode trunk** command, and then use the **switchport trunk** command to assign VLANs to the trunk. This switch port cannot pass traffic until you assign at least one VLAN to it. 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 trunk** command does not take effect unless the mode is set to trunk mode using the **switchport mode trunk** command.

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 seven VLAN interfaces, including the failover interface which is configured using the **failover lan** command. VLANs 200, 201, and 202 are trunked on Ethernet 0/1.

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 201
hostname(config-if)# nameif dept1
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 202
hostname(config-if)# nameif dept2
hostname(config-if)# security-level 90
hostname(config-if)# ip address 10.2.3.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

```
hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0

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 mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# switchport trunk native vlan 5
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
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 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)/8.0(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 ASA 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

The **tcp-map** command is used along with the Modular Policy Framework infrastructure. Define the class of traffic using the **class-map** command and customize the TCP inspection with **tcp-map** commands. Apply the new TCP map using the **policy-map** command. Activate TCP inspection with **service-policy** commands.

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **syn-data** command in tcp-map configuration mode to drop packets with data in SYN packets.

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 ASA 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)	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**.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

By default, the ASA allows VPN traffic to terminate on an ASA 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 ASA 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 **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 preserve-vpn-flows

To preserve and resume stateful (TCP) tunneled IPsec LAN-to-LAN traffic within the timeout period after the tunnel drops and recovers, use the **sysopt connection preserve-vpn-flows** command. To disable this feature, use the **no** form of this command.

sysopt connection preserve-vpn-flows

no sysopt connection preserve-vpn-flows

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
8.0(4)	This command was introduced.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

With the persistent IPsec tunneled flows feature enabled, as long as the tunnel is recreated within the timeout window, data continues flowing successfully because the security appliance still has access to the state information in the original flow.

This command supports only IPsec LAN-to-LAN tunnels, including Network Extension Mode. It does not support AnyConnect/SSL VPN or IPsec remote-access tunnels.

Examples

The following example specifies that the state information for the tunnel will be preserved and the tunneled IPsec LAN-to-LAN VPN traffic will resume after the tunnel drops and is reestablished within the timeout period:

```
hostname(config)# no sysopt connection preserve-vpn-flows
```

To see whether this feature is enabled, enter the show run all command for sysopt:

```
hostname(config)# show run all sysopt
```

A sample result follows. For illustrative purposes, in this and all following examples, the preserve-vpn-flows item is bolded:

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-vpn
no sysopt connection reclassify-vpn
no sysopt connection preserve-vpn-flows
hostname(config)#
```

sysopt connection reclassify-vpn

To reclassify existing VPN flows, use the **sysopt connection reclassify-vpn** command in global configuration mode. To disable this feature, use the **no** form of this command.

sysopt connection reclassify-vpn

no sysopt connection reclassify-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
8.0(2)	This command was introduced
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

When VPN tunnels come up, this command reclassifies existing VPN flows to make sure that flows that need encryption get torn down and recreated.

This command only applies for LAN-to-LAN and dynamic VPNs. This command has no effect on EZVPN or VPN client connections.

Examples

The following example enables VPN reclassification:

```
hostname(config)# sysopt connection reclassify-vpn
```

Related Commands

Command	Description
clear configure sysopt	Clears the **sysopt** command configuration.
show running-config sysopt	Shows the **sysopt** command configuration.
sysopt connection permit-vpn	Permits any packets that come from an IPsec tunnel without checking any acess lists for interfaces.

Command	Description
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 ASA 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 ASA 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 ASA alters the packet to request 1200 bytes (the maximum). If another host requests a maximum value of 300 bytes, then the ASA 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 ASA 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 ASA 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.

sysopt connection timewait

no sysopt connection timewait

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

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
7.0(1)	This command was introduced.

Usage Guidelines

The default behavior of the ASA 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 ASA 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 noproxyarp

To disable proxy ARP for NAT global addresses or VPN client addresses on an interface, use the **sysopt noproxyarp** command in global configuration mode. To reenable proxy ARP, 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 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
8.0(3)	This command was extended to affect VPN proxy ARPs when the VPN client addresses overlap with an internal network.

Usage Guidelines

If you have a VPN client address pool that overlaps with an existing network, the ASA by default sends proxy ARPs on all interfaces. If you have another interface that is on the same Layer 2 domain, it will see the ARP requests and will answer with the MAC address of its interface. The result of this is that the return traffic of the VPN clients towards the internal hosts will go to the wrong interface and will get dropped. In this case, you need to enter the **sysopt noproxyarp** command for the interface where you do not want proxy ARPs.

In rare circumstances, you might want to disable proxy ARP for NAT 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 ASA uses proxy ARP when you configure NAT and specify a global address that is on the same network as the ASA interface. The only way traffic can reach the hosts is if the ASA uses proxy ARP to claim that the ASA 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
7.0(1)	This command was introduced.

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 ASA 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.