CHAPTER 43

same-security-traffic through shape Commands

same-security-traffic

To permit communication between interfaces with equal security levels, or to allow traffic to enter and exit the same interface, use the **same-security-traffic** command in global configuration mode. To disable the same-security traffic, use the **no** form of this command.

same-security-traffic permit {**inter-interface** | **intra-interface**}

no same-security-traffic permit {**inter-interface** | **intra-interface**}

Syntax Description

inter-interface	Permits communication between different interfaces that have the same security level.
intra-interface	Permits communication in and out of the same interface.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	The **intra-interface** keyword now allows all traffic to enter and exit the same interface, and not just IPsec traffic.

Usage Guidelines

Allowing communication between same security interfaces (enabled by the **same-security-traffic inter-interface** command) provides the following benefits:

- You can configure more than 101 communicating interfaces. If you use different levels for each interface, you can configure only one interface per level (0 to 100).
- You can allow traffic to flow freely between all same security interfaces without access lists.

The **same-security-traffic intra-interface** command lets traffic enter and exit the same interface, which is normally not allowed. This feature might be useful for VPN traffic that enters an interface, but is then routed out the same interface. The VPN traffic might be unencrypted in this case, or it might be reencrypted for another VPN connection. For example, if you have a hub and spoke VPN network, where the ASA is the hub, and remote VPN networks are spokes, for one spoke to communicate with another spoke, traffic must go into the ASA and then out again to the other spoke.

Note All traffic allowed by the **same-security-traffic intra-interface** command is still subject to firewall rules. Be careful not to create an asymmetric routing situation that can cause return traffic not to traverse the ASA.

Examples

The following example shows how to enable the same-security interface communication:

```
hostname(config)# same-security-traffic permit inter-interface
```

The following example shows how to enable traffic to enter and exit the same interface:

```
hostname(config)# same-security-traffic permit intra-interface
```

Related Commands

Command	Description
show running-config same-security-traffic	Displays the **same-security-traffic** configuration.

sasl-mechanism

To specify a SASL (Simple Authentication and Security Layer) mechanism for authenticating an LDAP client to an LDAP server, use the **sasl-mechanism** command in aaa-server host configuration mode. The SASL authentication mechanism options are **digest-md5** and **kerberos**.

To disable an authentication mechanism, use the **no** form of this command.

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

Note Because the ASA serves as a client proxy to the LDAP server for VPN users, the LDAP client referred to here is the ASA.

Syntax Description

digest-md5	The ASA responds with an MD5 value computed from the username and password.
kerberos	The ASA responds by sending the username and realm using the GSSAPI (Generic Security Services Application Programming Interface) Kerberos mechanism.
server-group-name	Specifies the Kerberos aaa-server group, up to 64 characters.

Defaults

No default behavior or values. The ASA passes the authentication parameters to the LDAP server in plain text.

Note We recommend that you secure LDAP communications with SSL using the **ldap-over-ssl** command if you have not configured SASL.

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

Use this command to specify ASA authentication to an LDAP server using SASL mechanisms.

Both the ASA and the LDAP server can support multiple SASL authentication mechanisms. When negotiating SASL authentication, the ASA retrieves the list of SASL mechanisms configured on the server and sets the authentication mechanism to the strongest mechanism configured on both the ASA and the server. The Kerberos mechanism is stronger than the Digest-MD5 mechanism. To illustrate, if both the LDAP server and the ASA support both mechanisms, the ASA selects Kerberos, the stronger of the mechanisms.

When disabling the SASL mechanisms, you must enter a separate **no** command for each mechanism you want to disable because they are configured independently. Mechanisms that you do not specifically disable remain in effect. For example, you must enter both of the following commands to disable both SASL mechanisms:

no sasl-mechanism digest-md5

no sasl-mechanism kerberos <*server-group-name*>

Examples

The following examples, entered in aaa-server host configuration mode, enable the SASL mechanisms for authentication to an LDAP server named ldapsvr1 with an IP address of 10.10.0.1. This example enables the SASL digest-md5 authentication mechanism:

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
```

The following example enables the SASL Kerberos authentication mechanism and specifies kerb-servr1 as the Kerberos AAA server:

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
server-type	Specifies the LDAP server vendor as either Microsoft or Sun.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

sast

To specify the number of SAST certificates to create in the CTL record, use the **sast** command in ctl-file configuration mode. To set the number of SAST certificates in the CTL file back to the default value of 2, use the **no** form of this command.

sast *number_sasts*

no sast *number_sasts*

Syntax Description

number_sasts	Specifies the number of SAST keys to create. The default is 2. maximum allowed is 5.

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
Ctl-file configuration	•	—	•	—	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

CTL files are signed by a System Administrator Security Token (SAST).

Because the Phone Proxy generates the CTL file, it needs to create the SAST key to sign the CTL file itself. This key can be generated on the ASA. A SAST is created as a self-signed certificate.

Typically, a CTL file contains more than one SAST. In case a SAST is not recoverable, the other one can be used to sign the file later.

Examples

The following example shows the use of the **sast** command to create 5 SAST certificates in the CTL file:

```
hostname(config-ctl-file)# sast 5
```

Related Commands

Command	Description
ctl-file (global)	Specifies the CTL file to create for Phone Proxy configuration or the CTL file to parse from Flash memory.
ctl-file (phone-proxy)	Specifies the CTL file to use for Phone Proxy configuration.
phone-proxy	Configures the Phone Proxy instance.

scansafe

To enable Cloud Web Security inspection for a context, use the **scansafe** command in context configuration mode. To disable Cloud Web Security, use the **no** form of this command.

scansafe [**license** *key*]

no scansafe [**license** *key*]

Syntax Description

license *key*	Enters an authentication key for this context. If you do not specify a key, the context uses the license configured in the system configuration. The ASA sends the authentication key to the Cloud Web Security proxy servers to indicate from which organization the request comes. The authentication key is a 16-byte hexidecimal number.

Command Default

By default, the context uses the license entered in the system 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

In multiple context mode, you must allow Cloud Web Security per context.

Examples

The following sample configuration enables Cloud Web Security in context one with the default license and in context two with the license key override:

```
! System Context
!
scansafe general-options
server primary ip 180.24.0.62 port 8080
retry-count 5
license 366C1D3F5CE67D33D3E9ACEC265261E5
!
context one
 allocate-interface GigabitEthernet0/0.1
 allocate-interface GigabitEthernet0/1.1
 allocate-interface GigabitEthernet0/3.1
 scansafe
 config-url disk0:/one_ctx.cfg
!
context two
 allocate-interface GigabitEthernet0/0.2
 allocate-interface GigabitEthernet0/1.2
 allocate-interface GigabitEthernet0/3.2
 scansafe license 366C1D3F5CE67D33D3E9ACEC26789534
 config-url disk0:/two_ctx.cfg
!
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it’s the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

scansafe general-options

To configure communication with the Cloud Web Security proxy server, use the **scansafe general-options** command in global configuration mode. To remove the server configuration, use the **no** form of this command.

scansafe general-options

no scansafe general-options

Syntax Description

This command has no arguments or keywords.

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
Global configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

You can configure a primary and backup proxy server for Cloud Web Security.

Examples

The following example configures a primary server:

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.

Command	Description
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

scep-enrollment enable

To enable or disable the Simple Certificate Enrollment Protocol for a tunnel group, use the **scep-enrollment enable** command in tunnel-group general-attributes mode.

To remove the command from the configuration, use the **no** form of this command.

scep-enrollment enable

no scep-enrollment enable

Syntax Description

This command has no arguments or keywords.

Defaults

By default, this command is not present in the tunnel group 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**
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

Only the Cisco AnyConnect Secure Mobility Client, Release 3.0 and later, supports this feature.

The ASA can proxy SCEP requests between AnyConnect and a third-party certificate authority. The certificate authority only needs to be accessible to the ASA if it is acting as the proxy. For the ASA to provide this service, the user must authenticate using any of the methods supported by AAA before the ASA sends an enrollment request. You can also use Host Scan and dynamic access policies to enforce rules of eligibility to enroll.

The ASA supports this feature only with an AnyConnect SSL or IKEv2 VPN session. It supports all SCEP-compliant certificate authorities, including IOS CS, Windows Server 2003 CA, and Windows Server 2008 CA.

Clientless (browser-based) access does not support SCEP Proxy, although WebLaunch—clientless-initiated AnyConnect—does support it.

The ASA does not support polling for certificates.

The ASA supports load balancing for this feature.

Example

The following example, entered in global configuration mode, creates a remote access tunnel group named remotegrp and enables SCEP for the group policy:

```
hostname(config)# tunnel-group remotegrp type remote-access
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

Related Commands

Command	Description
crypto ikev2 enable	Enables IKEv2 negotiation on the interface on which IPsec peers communicate.
scep-forwarding-url	Enrolls the SCEP certificate authority for the group policy.
secondary-pre-fill-username clientless	Supplies a common, secondary password when a certificate is unavailable for WebLaunch support of the SCEP proxy.
secondary-authentication-server-group	Supplies the username when a certificate is unavailable.

scep-forwarding-url

To enroll an SCEP certificate authority for a group policy, use the **scep-forwarding-url** command in group-policy configuration mode.

To remove the command from the configuration, use the **no** form of this command.

scep-forwarding-url {**none** | **value** [*URL*]}

no scep-forwarding-url

Syntax Description

none	Specifies no certificate authority for the group policy.
URL	Specifies the SCEP URL of the certificate authority.
value	Enables this feature for clientless connections.

Defaults

By default, this command is not present.

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 configuration	•	—	•	—	—

Command History

Release	Modification
8.4(1)	This command was introduced.

Usage Guidelines

Enter this command once per group policy to support a third-party digital certificate.

Example

The following example, entered in global configuration mode, creates a group policy named FirstGroup and enrolls a certificate authority for the group policy:

```
hostname(config)# group-policy FirstGroup internal
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
Attempting to retrieve the CA/RA certificate(s) using the URL. Please wait ...
```

Related Commands

Command	Description
crypto ikev2 enable	Enables IKEv2 negotiation on the interface on which IPsec peers communicate.
scep-enrollment enable	Enables Simple Certificate Enrollment Protocol for a tunnel group.
secondary-pre-fill-username clientless	Supplies a common, secondary password when a certificate is unavailable for WebLaunch support of the SCEP proxy.
secondary-authentication-server-group	Supplies the username when a certificate is unavailable.

secondary

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

secondary

no secondary

Syntax Description

This command has no arguments or keywords.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

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

secondary-authentication-server-group

To specify a secondary authentication server group to associate with the session when double authentication is enabled, use the **secondary-authentication-server-group** command in tunnel-group general-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

secondary-authentication-server-group [*interface_name*] {**none** | **LOCAL** | *groupname* [**LOCAL**]} [**use-primary-username**] }

no secondary-authentication-server-group

Syntax Description

interface_name	(Optional) Specifies the interface where the IPsec tunnel terminates.
LOCAL	(Optional) Requires authentication against the local user database if all of the servers in the server group have been deactivated due to communication failures. If the server group name is either **LOCAL** or **NONE,** do not use the **LOCAL** keyword here.
none	(Optional) Specifies the server group name as **NONE**, indicating that authentication is not required.
groupname [**LOCAL**]	Identifies the previously configured authentication server or group of servers. Optionally, this can be the LOCAL group.
use-primary-username	Use the primary username as the username for the secondary authentication.

Defaults

The default value is **none**.

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
8.2(1)	This command was introduced.

Usage Guidelines

This command is meaningful only when double authentication is enabled. The **secondary-authentication-server-group** command specifies the secondary AAA server group. The secondary server group cannot be an SDI server group.

If the use-primary-username keyword is configured, then only one username is requested in the login dialog.

If the usernames are extracted from a digital certificate, only the primary username is used for authentication.

Examples

The following example, entered in global configuration mode, creates a remote access tunnel group named remotegrp and specifies the use of the group sdi_server as the primary server group and the group ldap_ server as the secondary authentication server group for the connection:

```
hostname(config)# tunnel-group remotegrp type remote-access
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-webvpn)# authentication-server-group sdi_server
hostname(config-tunnel-webvpn)# secondary-authentication-server-group ldap_server
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

secondary-color

To set a secondary color for the WebVPN login, home page, and file access page, use the **secondary-color** command in webvpn mode. To remove a color from the configuration and reset the default, use the **no** form of this command.

secondary-color [*color*]

no secondary-color

Syntax Description

color	(Optional) Specifies the color. You can use a comma separated RGB value, an HTML color value, or the name of the color if recognized in HTML. • RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others. • HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue. • Name length maximum is 32 characters

Defaults

The default secondary color is HTML #CCCCFF, a lavender shade.

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
7.0(1)	This command was introduced.

Usage Guidelines

The number of RGB values recommended for use is 216, many fewer than the mathematical possibilities. Many displays can handle only 256 colors, and 40 of those look differently on MACs and PCs. For best results, check published RGB tables. To find RGB tables online, enter RGB in a search engine.

Examples

The following example shows how to set an HTML color value of #5F9EAO, which is a teal shade:

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-color #5F9EAO
```

Related Commands

Command	Description
title-color	Sets a color for the WebVPN title bar on the login, home page, and file access page

secondary-pre-fill-username

To enable the extraction of a username from a client certificate for use in double authentication for a clientless or an AnyConnect connection, use the **secondary-pre-fill-username** command in tunnel-group webvpn-attributes mode. To remove the attribute from the configuration, use the **no** form of this command.

secondary-pre-fill-username {**clientless** | **ssl-client**} [**hide**]

secondary-pre-fill-username {**clientless** | **ssl-client**} **hide** [**use-primary-password** | **use-common-password** [*type_num*] *password*]

no secondary-no pre-fill-username

Syntax Description

clientless	Enables this feature for clientless connections.
hide	Hides the username to be used for authentication from the VPN user.
password	Enter the password string.
ssl-client	Enables this feature for AnyConnect VPN client connections.
type_num	Enter one of the following options: • 0 if the password to be entered is plain text. • 8 if the password to be entered is encrypted. The password appears as asterisks as you type.
use-common-password	Specifies a common secondary authentication password to use without prompting the user for it.
use-primary-password	Reuses the primary authentication password for secondary authentication without prompting the user for it.

Defaults

This feature is disabled by default. Entering this command without the **hide** keyword reveals the extracted username to the VPN user. The user receives a password prompt if you specify neither the **use-primary-password** nor the **use-common-password** keywords. The default value of *type_num* is 8.

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 webvpn-attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.2(1)	This command was introduced.
8.3(2)	Added [**use-primary-password** | **use-common-password** [*type_num*] *password*] to the command.

Usage Guidelines

To enable this feature, you must also enter the **secondary-username-from-certificate** command in tunnel-group general-attributes mode.

This command is meaningful only if double authentication is enabled. The **secondary-pre-fill-username** command enables the use of a username extracted from the certificate field specified in the **secondary-username-from-certificate** command as the username for secondary username/password authentication. To use this secondary-pre-fill username-from-certificate feature, you must configure both commands.

Note Clientless and SSL-client connections are not mutually exclusive options. Only one can be specified per command line, but both can be enabled at the same time.

If you hide the second username and use a primary or common password, the user experience is similar to single authentication. Using the primary or common password makes the use of device certificates to authenticate a device a seamless user experience.

The **use-primary-password** keyword specifies the use of the primary password as the secondary password for all authentications.

The **use-common-password** keyword specifies the use of a common secondary password for all secondary authentications. If a device certificate installed on the endpoint contains a BIOS ID or some other identifier, a secondary authentication request can use the pre-filled BIOS ID as the second username and use a common password configured for all authentications in that tunnel group.

Examples

The following example creates an IPsec remote access tunnel group named remotegrp, and specifies the reuse of a name from the digital certificate on the endpoint as the name to be used for an authentication or authorization query when the connections are browser-based.

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)# secondary-pre-fill-username clientless
```

The following example performs the same function as the previous command, but hides the extracted username from the user:

```
hostname(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
```

The following example performs the same function as the previous command, except that it applies only to AnyConnect connections:

```
hostname(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
```

The following example hides the username and reuses the primary authentication password for secondary authentication without prompting the user:

```
hostname(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-primary-password
```

The following example hides the username and uses the password you enter for secondary authentication:

```
hostname(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password **********
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
tunnel-group general-attributes	Specifies the general attributes for the named tunnel-group.
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.

secondary-text-color

To set the secondary text color for the WebVPN login, home page and file access page, use the **secondary-text-color** command in webvpn mode. To remove the color from the configuration and reset the default, use the **no** form of this command.

secondary-text-color [*black* | *white*]

no secondary-text-color

Syntax Description

auto	Chooses black or white based on the settings for the text-color command. That is, if the primary color is black, this value is white.
black	The default secondary text color is black.
white	You can change the text color to white.

Defaults

The default secondary text color is black.

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
7.0(1)	This command was introduced.

Examples

The following example shows how to set the secondary text color to white:

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-text-color white
```

Related Commands

Command	Description
text-color	Sets a color for text in the WebVPN title bar on the login, home page and file access page

secure-unit-authentication

To enable secure unit authentication, use the **secure-unit-authentication enable** command in group-policy configuration mode. To disable secure unit authentication, use the **secure-unit-authentication disable** command. To remove the secure unit authentication attribute from the running configuration, use the **no** form of this command. **secure-unit-authentication** {**enable** | **disable**}

no secure-unit-authentication

Syntax Description

disable	Disables secure unit authentication.
enable	Enables secure unit authentication.

Defaults

Secure unit authentication 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 configuration	•	—	•	—	—

Command History

Release	**Modification**
7.0(1)	This command was introduced.

Usage Guidelines

Secure unit authentication requires that you have an authentication server group configured for the tunnel group the hardware client(s) use.

If you require secure unit authentication on the primary ASA, be sure to configure it on any backup servers as well.

The **no** option allows inheritance of a value for secure unit authentication from another group policy.

Secure unit authentication provides additional security by requiring VPN hardware clients to authenticate with a username and password each time the client initiates a tunnel. With this feature enabled, the hardware client does not have a saved username and password.

Note With this feature enabled, to bring up a VPN tunnel, a user must be present to enter the username and password.

Examples

The following example shows how to enable secure unit authentication for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN hardware client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
user-authentication	Requires users behind a hardware client to identify themselves to the ASA before connecting.

secondary-username-from-certificate

To specify the field in a certificate to use as the secondary username for double authentication for a clientless or AnyConnect (SSL-client) connection, use the **secondary-username-from-certificate** command in tunnel-group general-attributes mode.

To remove the attribute from the configuration and restore default values, use the **no** form of this command.

secondary-username-from-certificate {*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**}

no secondary-username-from-certificate

Syntax Description

primary-attr	Specifies the attribute to use to derive a username for an authorization query from a certificate. If pre-fill-username is enabled, the derived name can also be used in an authentication query.
secondary-attr	(Optional) Specifies an additional attribute to use with the primary attribute to derive a username for an authentication or authorization query from a digital certificate. If pre-fill-username is enable, the derived name can also be used in an authentication query.
use-entire-name	Specifies that the ASA must use the entire subject DN (RFC1779) to derive a name for an authorization query from a digital certificate.
use-script	Specifies the use of a script file generated by ASDM to extract the DN fields from a certificate for use as a username.

Defaults

This feature is disabled by default and is meaningful only when double authentication 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
Tunnel-group general-attributes configuration	•	—	•	—	—

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

This command is meaningful only when double authentication is enabled.

When double authentication is enabled. this command selects one or more fields in a certificate to use as the username. The **secondary-username-from-certificate** command forces the security appliance to use the specified certificate field as the second username for the second username/password authentication.

To use this derived username in the pre-fill username from certificate feature for the secondary username/password authentication or authorization, you must also configure the **pre-fill-username** and **secondary-pre-fill-username** commands in tunnel-group webvpn-attributes mode. That is, to use the secondary pre-fill username feature, you must configure both commands.

Possible values for primary and secondary attributes include the following:

Attribute	Definition
C	Country: the two-letter country abbreviation. These codes conform to ISO 3166 country abbreviations.
CN	Common Name: the name of a person, system, or other entity. Not available a s a secondary attribute.
DNQ	Domain Name Qualifier.
EA	E-mail address.
GENQ	Generational Qualifier.
GN	Given Name.
I	Initials.
L	Locality: the city or town where the organization is located.
N	Name.
O	Organization: the name of the company, institution, agency, association or other entity.
OU	Organizational Unit: the subgroup within the organization (O).
SER	Serial Number.
SN	Surname.
SP	State/Province: the state or province where the organization is located
T	Title.
UID	User Identifier.
UPN	User Principal Name.
use-entire-name	Use entire DN name. Not available a s a secondary attribute.
use-script	Use a script file generated by ASDM.

Note If you also specify the **secondary-authentication-server-group** command, along with the **secondary-username-from-certificate command, only** the primary username is used for authentication.

Examples

The following example, entered in global configuration mode, creates a remote access tunnel group named remotegrp and specifies the use of CN (Common Name) as the primary attribute and OU as the secondary attribute to use to derive a name for an authorization query from a digital certificate:

```
hostname(config)# tunnel-group remotegrp type remote-access
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# username-from-certificate CN
hostname(config-tunnel-general)# secondary-username-from-certificate OU
hostname(config-tunnel-general)#
```

The following example shows how to modify the tunnel-group attributes to configure the pre-fill username.

```
username-from-certificate {use-entire-name | use-script | <primary-attr>} [secondary-attr]
secondary-username-from-certificate {use-entire-name | use-script | <primary-attr>}
[secondary-attr] ; used only for double-authentication
```

Related Commands

Command	Description
pre-fill-username	Enables the pre-fill username feature.
secondary-pre-fill-username	Enables username extraction for clientless or AnyConnect client connection
username-from-certificate	Specifies the field in a certificate to use as the username for authorization.
show running-config tunnel-group	Shows the indicated tunnel-group configuration.
secondary-authentication-server-group	Specifies the secondary AAA server group. If the usernames are extracted from a digital certificate, only the primary username is used for authentication.

security-group

To add a security group to a security object group for use with Cisco TrustSec, use the **security-group** command in object-group security configuration mode. To remove the security group, use the **no** form of this command.

security-group {**tag** *sgt#* | **name** *sg_name*}

no security-group {**tag** *sgt#* | **name** *sg_name*}

Syntax Description

tag *sgt#*	Specifies the security group object as an inline tag. Enter a number from 1 to 65533 for a Tag security type. An SGT is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB) by the ISE. Security group names are created on the ISE and provide user-friendly names for security groups. The security group table maps SGTs to security group names.
name *sg_name*	Specifies the security group object as a named object. Enter a 32-byte case-sensitive string for a Name security type. The *sg_name* can contain any character including [a-z], [A-Z], [0-9], [!@#$%^&()-_{}.].

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
Object-group security configuration	•	•	•	•	—

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

You can create security group object groups for use in features that support Cisco TrustSec by including the group in an extended ACL, which in turn can be used in an access rule, for example.

When integrated with Cisco TrustSec, the ASA downloads security group information from the ISE. The ISE acts as an identity repository, by providing Cisco TrustSec tag to user identity mapping and Cisco TrustSec tag to server resource mapping. You provision and manage security group access lists centrally on the ISE.

However, the ASA might have localized network resources that are not defined globally that require local security groups with localized security policies. Local security groups can contain nested security groups that are downloaded from the ISE. The ASA consolidates local and central security groups.

To create local security groups on the ASA, you create a local security object group. A local security object group can contain one or more nested security object groups or Security IDs or security group names. User can also create a new Security ID or security group name that does not exist on the ASA.

You can use the security object groups you create on the ASA to control access to network resources. You can use the security object group as part of an access group or service policy.

Examples

The following example shows how to configure a security group object:

```
hostname(config)# object-group security mktg-sg
hostname(config)# security-group name mktg
hostname(config)# security-group tag 1
```

The following example shows how to configure a security group object:

```
hostname(config)# object-group security mktg-sg-all
hostname(config)# security-group name mktg-managers
hostname(config)# group-object mktg-sg // nested object-group
```

Related Commands

Command	Description
object-group security	Creates a security group object.

security-level

To set the security level of an interface, use the **security-level** command in interface configuration mode. To set the security level to the default, use the **no** form of this command. The security level protects higher security networks from lower security networks by imposing additional protection between the two.

security-level *number*

no security-level

Syntax Description

number	An integer between 0 (lowest) and 100 (highest).

Defaults

By default, the security level is 0.

If you name an interface "inside" and you do not set the security level explicitly, then the ASA sets the security level to 100 (see the **nameif** command). You can change this level if desired.

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 **nameif** command to an interface configuration mode command.

Usage Guidelines

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

  For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

- Inspection engines—Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
  - NetBIOS inspection engine—Applied only for outbound connections.
  - OraServ inspection engine—If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the ASA.

- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

  For same security interfaces, you can filter traffic in either direction.
- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

  Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.
- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

  For same security interfaces, you can configure **established** commands for both directions.

Normally, interfaces on the same security level cannot communicate. If you want interfaces on the same security level to communicate, see the **same-security-traffic** command. You might want to assign two interfaces to the same level and allow them to communicate if you want to create more than 101 communicating interfaces, or you want protection features to be applied equally for traffic between two interfaces; for example, you have two departments that are equally secure.

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Examples

The following example configures the security levels for two interfaces to be 100 and 0:

```
hostname(config)# interface gigabitethernet0/0
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
hostname(config-if)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear local-host	Resets all connections.
interface	Configures an interface and enters interface configuration mode.
nameif	Sets the interface name.
vlan	Assigns a VLAN ID to a subinterface.

send response

To send a RADIUS Accounting-Response Start and Accounting-Response Stop message to the sender of the RADIUS Accounting-Request Start and Stop messages, use the **send response** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command.

This option is disabled by default.

send response

no send response

Syntax Description

This command has no arguments or keywords.

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
Radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to send a response with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# send response
hostname(config-pmap-p)# send response
```

Related Commands

Commands	Description
inspect radius-accounting	Sets inspection for RADIUS accounting.
parameters	Sets parameters for an inspection policy map.

seq-past-window

To set the action for packets that have past-window sequence numbers (the sequence number of a received TCP packet is greater than the right edge of the TCP receiving window), use the **seq-past-window** 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.

seq-past-window {**allow** | **drop**}

no seq-past-window

Syntax Description

allow	Allows packets that have past-window sequence numbers. This action is only allowed if the **queue-limit** command is set to 0 (disabled).
drop	Drops packets that have past-window sequence numbers.

Defaults

The default action is to drop packets that have past-window sequence numbers.

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. **seq-past-window**—In tcp-map configuration mode, you can enter the **seq-past-window** 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 packets that have past-window sequence numbers:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# seq-past-window 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.
queue-limit	Sets the out-of-order packet limit.
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.

serial-number

To include the ASA serial number in the certificate during enrollment, use the **serial-number** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

serial-number

no serial-number

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is to not include the serial number.

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 includes the ASA serial number in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

server (pop3s, imap4s, smtps)

To specify a default e-mail proxy server, use the **server** command in the applicable e-mail proxy configuration mode. To remove the attribute from the configuration, use the **no** version of this command. The ASA sends requests to the default e-mail server when the user connects to the e-mail proxy without specifying a server. If you do not configure a default server, and a user does not specify a server, the ASA returns an error.

server {*ipaddr or hostname*}

no server

Syntax Description

hostname	The DNS name of the default e-mail proxy server.
ipaddr	The IP address of the default e-mail proxy server.

Defaults

There is no default e-mail proxy server 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
Pop3s configuration	•	•	—	—	•
Imap4s configuration	•	•	—	—	•
Smtps configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to set a default POP3S e-mail server with an IP address. of 10.1.1.7:

```
hostname(config)# pop3s
hostname(config-pop3s)# server 10.1.1.7
```

server authenticate-client

To enable the ASA to authenticate the TLS client during TLS handshake, use the **server authenticate-client** command in tls-proxy configuration mode.

To bypass client authenticaion, use the **no** form of this command.

server authenticate-client

no server authenticate-client

Syntax Description

This command has arguments or keywords.

Defaults

This command is enabled by default, which means the TLS client is required to present a certificate during handshake with the ASA.

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
Tls-proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

Use the **server authenticate-client** command to control whether a client authentication is required during TLS Proxy handshake. When enabled (by default), the security appliance sends a Certificate Request TLS handshake message to the TLS client, and the TLS client is required to present its certificate.

Use the **no** form of this command to disable client authentication. Disabling TLS client authentication is suitable when the ASA must interoperate with CUMA client or clients such as a Web browser that are incapable of sending a client certificate.

Examples

The following example configures a TLS proxy instance with client authentication disabled:

```
hostname(config)# tls-proxy mmp_tls
hostname(config-tlsp)# no server authenticate-client
hostname(config-tlsp)# server trust-point cuma_server_proxy
```

Related Commands

Command	Description
tls-proxy	Configures the TLS proxy instance.

server backup

To configure the backup Cloud Web Security proxy server, use the **server backup** command in scansafe general-options configuration mode. To remove the server, use the **no** form of this command.

server backup {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server backup [**ip** *ip_address* | **fqdn** *fqdn*] [**port** *port*]

Syntax Description

ip *ip_address*	Specifies the server IP address.
fqdn *fqdn*	Specifies the server fully-qualified domain name (FQDN).
port *port*	(Optional) By default, the Cloud Web Security proxy server uses port 8080 for both HTTP and HTTPS traffic; do not change this value unless directed to do so.

Command Default

The default port is 8080.

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
Scansafe general-options configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server. See the **server primary** command to configure the primary server. These servers are routinely polled to check for their availability. If your ASA is unable to reach the Cloud Web Security proxy server (for example, if no SYN/ACK packets arrive from the proxy server), then the proxy server is polled through a TCP three-way handshake to check its availability. If the proxy server is unavailable after a configured number of retries (default is five), the server is declared as unreachable, and the backup proxy server becomes active.

The ASA automatically falls back to the primary Cloud Web Security proxy server from the backup server after continued polling shows that the primary server is active for two consecutive retry count periods. You can change this polling interval using the **retry-count** command.

Traffic Conditions Under Which Proxy Server Is Not Reachable	Server Timeout Calculation	Connection Timeout Result
High traffic	Client half open connection timeout + ASA TCP connection timeout	(30 + 30) = 60 seconds
Single connection failure	Client half open connection timeout + ((retry threshold - 1) x (ASA TCP connection timeout))	(30 + ((5-1) x (30)) = 150 seconds
Idle—No connections are passing	15 minutes + ((retry threshold) x (ASA TCP connection timeout))	900 + (5 x (30) = 1050 seconds

Examples

The following example configures a primary and backup server:

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.
show scansafe statistics	Shows total and current http connections.

Command	Description
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

server primary

To configure the primary Cloud Web Security proxy server, use the **server primary** command in scansafe general-options configuration mode. To remove the server, use the **no** form of this command.

server primary {**ip** *ip_address* | **fqdn** *fqdn*} [**port** *port*]

no server primary [**ip** *ip_address* | **fqdn** *fqdn*] [**port** *port*]

Syntax Description

ip *ip_address*	Specifies the server IP address.
fqdn *fqdn*	Specifies the server fully-qualified domain name (FQDN).
port *port*	(Optional) By default, the Cloud Web Security proxy server uses port 8080 for both HTTP and HTTPS traffic; do not change this value unless directed to do so.

Command Default

The default port is 8080.

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
Scansafe general-options configuration	•	•	•	—	•

Command History

Release	Modification
9.0(1)	We introduced this command.

Usage Guidelines

When you subscribe to the Cisco Cloud Web Security service, you are assigned a primary Cloud Web Security proxy server and backup proxy server. See the **server backup** command to configure the backup server. These servers are routinely polled to check for their availability. If your ASA is unable to reach the Cloud Web Security proxy server (for example, if no SYN/ACK packets arrive from the proxy server), then the proxy server is polled through a TCP three-way handshake to check its availability. If the proxy server is unavailable after a configured number of retries (default is five), the server is declared as unreachable, and the backup proxy server becomes active.

The ASA automatically falls back to the primary Cloud Web Security proxy server from the backup server after continued polling shows that the primary server is active for two consecutive retry count periods. You can change this polling interval using the **retry-count** command.

Traffic Conditions Under Which Proxy Server Is Not Reachable	Server Timeout Calculation	Connection Timeout Result
High traffic	Client half open connection timeout + ASA TCP connection timeout	(30 + 30) = 60 seconds
Single connection failure	Client half open connection timeout + ((retry threshold - 1) x (ASA TCP connection timeout))	(30 + ((5-1) x (30)) = 150 seconds
Idle—No connections are passing	15 minutes + ((retry threshold) x (ASA TCP connection timeout))	900 + (5 x (30) = 1050 seconds

Examples

The following example configures a primary and backup server:

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

Related Commands

Command	Description
class-map type inspect scansafe	Creates an inspection class map for whitelisted users and groups.
default user group	Specifies the default username and/or group if the ASA cannot determine the identity of the user coming into the ASA.
http[**s**] (parameters)	Specifies the service type for the inspection policy map, either HTTP or HTTPS.
inspect scansafe	Enables Cloud Web Security inspection on the traffic in a class.
license	Configures the authentication key that the ASA sends to the Cloud Web Security proxy servers to indicate from which organization the request comes.
match user group	Matches a user or group for a whitelist.
policy-map type inspect scansafe	Creates an inspection policy map so you can configure essential parameters for the rule and also optionally identify the whitelist.
retry-count	Enters the retry counter value, which is the amount of time that the ASA waits before polling the Cloud Web Security proxy server to check its availability.
scansafe	In multiple context mode, allows Cloud Web Security per context.
scansafe general-options	Configures general Cloud Web Security server options.
server {**primary** | **backup**}	Configures the fully qualified domain name or IP address of the primary or backup Cloud Web Security proxy servers.
show conn scansafe	Shows all Cloud Web Security connections, as noted by the capitol Z flag.
show scansafe server	Shows the status of the server, whether it's the current active server, the backup server, or unreachable.

Command	Description
show scansafe statistics	Shows total and current HTTP(S) connections.
user-identity monitor	Downloads the specified user or group information from the AD agent.
whitelist	Performs the whitelist action on the class of traffic.

server trust-point

To specify the proxy trustpoint certificate to present during TLS handshake, use the **server trust-point** command in TLS server configuration mode.

server trust-point *proxy_trustpoint*

Syntax Description

proxy_trustpoint	Specifies the trustpoint defined by the **crypto ca trustpoint** command.

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
TLS-proxy configuration	•	•	•	•	—

Command History

Release	Modification
8.0(4)	The command was introduced.

Usage Guidelines

The trustpoint can be self-signed, enrolled with a certificate authority, or from an imported credential. The **server trust-point** command has precedence over the global **ssl trust-point** command.

The **server trust-point** command specifies the proxy trustpoint certificate presented during TLS handshake. The certificate must be owned by the ASA (identity certificate). The certificate can be self-signed, enrolled with a certificate authority, or from an imported credential.

Create TLS proxy instances for each entity that can initiate a connection. The entity that initiates the TLS connection is in the role of TLS client. Because the TLS Proxy has strict definition of client proxy and server proxy, two TLS proxy instances must be defined if either of the entities could initiate the connection.

Note When you are creating the TLS proxy instance to use with the Phone Proxy, the server trustpoint is the internal Phone Proxy trustpoint created the CTL file instance. The trustpoint name is in the form *internal_PP_<ctl-file_instance_name>*

Examples

The following example shows the use of the **server trust-point** command to specify the proxy trustpoint certificate to present during TLS handshake:

```
hostname(config-tlsp)# server trust-point ent_y_proxy
```

Related Commands

Command	Description
client (tls-proxy)	Configures trustpoints, keypairs, and cipher suites for a TLS proxy instance.
client trust-point	Specifies the proxy trustpoint certificate to present during TLS handshake.
ssl trust-point	Specifies the certificate trustpoint that represents the SSL certificate for an interface.
tls-proxy	Configures a TLS proxy instance.

server-port

To configure a AAA server port for a host, use the **server-port** command in aaa-server host mode. To remove the designated server port, use the **no** form of this command.

server-port *port-number*

no server-port *port-number*

Syntax Description

port-number	A port number in the range of 0 through 65535.

Defaults

The default server ports are as follows:

- SDI—5500
- LDAP—389
- Kerberos—88
- NT—139
- TACACS+—49

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 group	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example configures an SDI AAA server named srvgrp1 to use server port number 8888:

```
hostname(config)# aaa-server srvgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# server-port 8888
```

Related Commands

Command	Description
aaa-server host	Configures host-specific AAA server parameters.

clear configure aaa-server	Removes all AAA server configurations.
show running-config aaa-server	Displays AAA server statistics for all AAA servers, for a particular server group, for a particular server within a particular group, or for a particular protocol.

server-separator

To specify a character as a delimiter between the e-mail and VPN server names, use **server-separator** command in the applicable e-mail proxy mode. To revert to the default, ":", use the no form of this command.

server-separator {*symbol*}

no server-separator

Syntax Description

symbol	The character that separates the e-mail and VPN server names. Choices are "@," (at) "l" (pipe), ":"(colon), "#" (hash), "," (comma), and ";" (semi-colon).

Defaults

The default is "@" (at).

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
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The server separator must be different from the name separator.

Examples

The following example shows how to set a pipe (|) as the server separator for IMAP4S:

```
hostname(config)# imap4s
hostname(config-imap4s)# server-separator |
```

Related Commands

Command	Description
name-separator	Separates the e-mail and VPN usernames and passwords.

server-type

To manually configure the LDAP server model, use the **server-type** command in aaa-server host configuration mode. The ASA supports the following server models:

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server, formerly named the Sun ONE Directory Server
- Generic LDAP directory servers that comply with LDAPv3 (no password management)

To disable this command, use the **no** form of this command.

server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

no server-type {**auto-detect** | **microsoft** | **sun** | **generic** | **openldap** | **novell**}

Syntax Description

auto-detect	Specifies that the ASA determines the LDAP server type through auto-detection.
generic	Specifies LDAP v3-compliant directory servers other than Sun and Microsoft LDAP directory servers. Password management is not supported with generic LDAP servers.
microsoft	Specifies that the LDAP server is a Microsoft Active Directory.
openldap	Specifies that the LDAP server is an OpenLDAP server.
novell	Specifies that the LDAP server is a Novell server.
sun	Specifies that the LDAP server is a Sun Microsystems JAVA System Directory Server.

Defaults

By default, auto-detection attempts to determine the server type.

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.
8.0(2)	Support for the OpenLDAP and Novell server types was added.

Usage Guidelines

The ASA supports LDAP version 3 and is compatible with the Sun Microsystems JAVA System Directory Server, the Microsoft Active Directory, and other LDAPv3 directory servers.

Note

- Sun—The DN configured on the ASA to access a Sun directory server must be able to access the default password policy on that server. We recommend using the directory administrator, or a user with directory administrator privileges, as the DN. Alternatively, you can place an ACI on the default password policy.
- Microsoft—You must configure LDAP over SSL to enable password management with Microsoft Active Directory.
- Generic—Password management features are not supported.

By default, the ASA auto-detects whether it is connected to a Microsoft directory server, a Sun LDAP directory server, or a generic LDAPv3 server. However, if auto-detection fails to determine the LDAP server type and if you know the server is either a Microsoft or Sun server, you can use the **server-type** command to manually configure the server as either a Microsoft or a Sun Microsystems LDAP server.

Examples

The following example, entered in aaa-server host configuration mode, configures the server type for the LDAP server ldapsvr1 at IP address 10.10.0.1. The first example configures a Sun Microsystems LDAP server.

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type sun
```

The following example specifies that the ASA use auto-detection to determine the server type:

```
hostname(config)# aaa-server ldapsvr1 protocol LDAP
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type auto-detect
```

Related Commands

Command	Description
ldap-over-ssl	Specifies that SSL secures the LDAP client-server connection.
sasl-mechanism	Configures SASL authentication between the LDAP client and server.
ldap attribute-map (global configuration mode)	Creates and names an LDAP attribute map for mapping user-defined attribute names to Cisco LDAP attribute names.

service

To enable resets for denied TCP connections, use the **service** command in global configuration mode. To disable resets, use the **no** form of this command.

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

Syntax Description

interface *interface_name*	Enables or disables resets for the specified interface.
resetinbound	Sends TCP resets for all inbound TCP sessions that attempt to transit the ASA and are denied by the ASA based on access lists or AAA settings. The ASA also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. Traffic between same security level interfaces is also affected. When this option is not enabled, the ASA silently discards denied packets. If you do not specify an interface, then this setting applies to all interfaces.
resetoutbound	Sends TCP resets for all outbound TCP sessions that attempt to transit the ASA and are denied by the ASA based on access lists or AAA settings. The ASA also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. Traffic between same security level interfaces is also affected. When this option is not enabled, the ASA silently discards denied packets. This option is enabled by default. You might want to disable outbound resets to reduce the CPU load during traffic storms, for example.
resetoutside	Enables resets for TCP packets that terminate at the least secure interface and are denied by the ASA based on access lists or AAA settings. The ASA also sends resets for packets that are allowed by an access list or AAA, but do not belong to an existing connection and are denied by the stateful firewall. When this option is not enabled, the ASA silently discards the packets of denied packets. We recommend that you use the **resetoutside** keyword with interface PAT. This keyword allows the ASA to terminate the IDENT from an external SMTP or FTP server. Actively resetting these connections avoids the 30-second timeout delay.

Defaults

By default, **service resetoutbound** is enabled for all interfaces.

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
7.1(1)	The **interface** keyword and the **resetoutbound** command were added.

Usage Guidelines

You might want to explicitly send resets for inbound traffic if you need to reset identity request (IDENT) connections. When you send a TCP RST (reset flag in the TCP header) to the denied host, the RST stops the incoming IDENT process so that you do not have to wait for IDENT to time out. Waiting for IDENT to time out can cause traffic to slow because outside hosts keep retransmitting the SYN until the IDENT times out, so the **service resetinbound** command might improve performance.

Examples

The following example disables outbound resets for all interfaces except for the inside interface:

```
hostname(config)# no service resetoutbound
hostname(config)# service resetoutbound interface inside
```

The following example enables inbound resets for all interfaces except for the DMZ interface:

```
hostname(config)# service resetinbound
hostname(config)# no service resetinbound interface dmz
```

The following example enables resets for connections that terminate on the outside interface:

```
hostname(config)# service resetoutside
```

Related Commands

Command	Description
show running-config service	Displays the service configuration.

service (ctl-provider)

To specify the port to which the Certificate Trust List provider listens, use the **service** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

service port *listening_port*

no service port *listening_port*

Syntax Description

port *listening_port*	Specifies the certificate to be exported to the client.

Defaults

Default port is 2444.

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
Ctl provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **service** command in CTL provider configuration mode to specify the port to which the CTL provider listens. The port must be the one listened to by the CallManager servers in the cluster (as configured under Enterprise Parameters on the CallManager administration page). The default port is 2444.

Examples

The following example shows how to create a CTL provider instance:

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

Related Commands

Commands	Description
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.
ctl	Parses the CTL file from the CTL client and install trustpoints.

Commands	Description
ctl-provider	Configures a CTL provider instance in CTL provider mode.
export	Specifies the certificate to be exported to the client
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

service (object service)

To define the protocol and optional port for a service object, use the **service** command in object service configuration mode. Use the **no** form of this command to remove the definition.

service {*protocol* | {**tcp** | **udp**} [**source** *operator number*] [**destination** *operator number*] | **icmp** [*icmp_type*] | **icmp6** [*icmp6_type*]}

no service {*protocol* | {**tcp** | **udp**} [**source** *operator number*] [**destination** *operator number*] | **icmp** [*icmp_type*] | **icmp6** [*icmp6_type*]}

Syntax Description

destination *operator number*	(Optional) For **tcp** and **udp** protocols, specifies the destination port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **eq**—Equals the port number. • **gt**—Greater than the port number. • **lt**—Less than the port number. • **neq**—Not equal to the port number. • **range**—A range of ports. Specify two numbers separated by a space, such as **range 1024 4500**.
icmp [*icmp_type*]	Specifies that the service type is for ICMP connections. You can optionally specify the ICMP type by name or number, between 0 and 255. For available optional ICMP type names, see the CLI help.
icmp6 [*icmp6_type*]	Specifies that the service type is for ICMP version 6 connections. You can optionally specify the ICMPv6 type by name or number, between 0 and 255. For available optional ICMPv6 type names, see the CLI help.
protocol	Identifies the protocol name or number, between 0 and 255. For a list of supported names, see the CLI help.
source *operator number*	(Optional) For **tcp** and **udp** protocols, specifies the source port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **eq**—Equals the port number. • **gt**—Greater than the port number. • **lt**—Less than the port number. • **neq**—Not equal to the port number. • **range**—A range of ports. Specify two numbers separated by a space, such as **range 1024 4500**.
tcp	Specifies that the service type is for TCP connections.
udp	Specifies that the service type is for UDP connections.

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 service configuration	•	•	•	•	—

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

You can use service objects by name in other parts of your configuration, for example ACLs (the **access-list** command) and NAT (the **nat** command).

If you configure an existing service object with a different protocol and port, the new configuration replaces the existing protocol and port with the new ones.

Examples

The following example shows how to create a service object for SSH traffic:

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh
```

The following example shows how to create a service object for EIGRP traffic:

```
hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp
```

The following example shows how to create a service object for traffic coming from port 0 through 1024 to HTTPS:

```
hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
object-group service	Configures a service object.
show running-config object service	Shows the current service object configuration.

service call-home

To enable the Call Home service, use the **service call-home** command in global configuration mode. To disable the Call Home service, use the **no** form of this command.

service call-home

no service call-home

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the service Call Home 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
Global configuration	•	•	•	—	•

Command History

Release	Modification
8.2(2)	This command was introduced.

Examples

The following example shows how to enable the Call Home service:

```
hostname(config)# service call-home
```

The followingexample shows how to disable the Call Home service:

```
hostname(config)# no service call-home
```

Related Commands

Command	Description
call-home (global configuration)	Enters Call Home configuration mode.
call-home test	Manually sends a Call Home test message.
show call-home	Displays Call Home configuration information.

service password-recovery

To enable password recovery, use the **service password-recovery** command in global configuration mode. To disable password recovery, use the **no** form of this command. Password recovery is enabled by default, but you might want to disable it to ensure that unauthorized users cannot use the password recovery mechanism to compromise the ASA.

service password-recovery

no service password-recovery

Syntax Description

This command has no arguments or keywords.

Defaults

Password recovery 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 was introduced.

Usage Guidelines

On the ASA 5500 series adaptive security appliance, if you forget the passwords, you can boot the ASA into ROMMON by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then set the ASA to ignore the startup configuration by changing the configuration register (see the **config-register** command). For example if your configuration register is the default 0x1, then change the value to 0x41 by entering the **confreg 0x41** command. After reloading the ASA, it loads a default configuration, and you can enter privileged EXEC mode using the default passwords. Then load the startup configuration by copying it to the running configuration and reset the passwords. Finally, set the ASA to boot as before by setting the configuration register to the original setting. For example, enter the **config-register 0x1** command in global configuration mode.

On the PIX 500 series security appliance, boot the ASA into monitor mode by pressing the **Escape** key on the terminal keyboard when prompted during startup. Then download the PIX password tool to the ASA, which erases all passwords and **aaa authentication** commands.

On the ASA 5500 series adaptive security appliance, the **no service password-recovery** command prevents a user from entering ROMMON with the configuration intact. When a user enters ROMMON, the ASA prompts the user to erase all Flash file systems. The user cannot enter ROMMON without first performing this erasure. If a user chooses not to erase the Flash file system, the ASA reloads. Because password recovery depends on using ROMMON and maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available. The **service password-recovery** command appears in the configuration file for informational purposes only; when you enter the command at the CLI prompt, the setting is saved in NVRAM. The only way to change the setting is to enter the command at the CLI prompt. Loading a new configuration with a different version of the command does not change the setting. If you disable password recovery when the ASA is configured to ignore the startup configuration at startup (in preparation for password recovery), then the ASA changes the setting to boot the startup configuration as usual. If you use failover, and the standby unit is configured to ignore the startup configuration, then the same change is made to the configuration register when the **no service password recovery** command replicates to the standby unit.

On the PIX 500 series security appliance, the **no service password-recovery** command forces the PIX password tool to prompt the user to erase all Flash file systems. The user cannot use the PIX password tool without first performing this erasure. If a user chooses not to erase the Flash file system, the ASA reloads. Because password recovery depends on maintaining the existing configuration, this erasure prevents you from recovering a password. However, disabling password recovery prevents unauthorized users from viewing the configuration or inserting different passwords. In this case, to recover the system to an operating state, load a new image and a backup configuration file, if available.

Examples

The following example disables password recovery for the ASA 5500 series:

```
hostname(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including configuration
files and images.  You should make a backup of your configuration and have a mechanism to
restore images from the ROMMON command line.
```

The following example for the ASA 5500 series shows when to enter ROMMON at startup and how to complete a password recovery operation.

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
###################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
```

```
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

Related Commands

Command	Description
config-register	Sets the ASA to ignore the startup configuration when it reloads.
enable password	Sets the enable password.
password	Sets the login password.

service-object

To add a service or service object to a service object group that is not pre-defined as TCP, UDP, or TCP-UDP, use the **service-object** command in object-group service configuration mode. To remove a service, use the **no** form of this command.

service-object {*protocol* | {**tcp** | **udp** | **tcp-udp**} [**source** *operator number*] [**destination** *operator number*] | **icmp** [*icmp_type*] | **icmp6** [*icmp6_type*] | **object** *name*}

no service-object {*protocol* | {**tcp** | **udp** | **tcp-udp**} [**source** *operator number*] [**destination** *operator number*] | **icmp** [*icmp_type*] | **icmp6** [*icmp6_type*] | **object** *name*}

Syntax Description

destination *operator number*	(Optional) For **tcp**, **udp**, or **tcp-udp** protocols, specifies the destination port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **eq**—Equals the port number. • **gt**—Greater than the port number. • **lt**—Less than the port number. • **neq**—Not equal to the port number. • **range**—A range of ports. Specify two numbers separated by a space, such as **range 1024 4500**.
icmp [*icmp_type*]	Specifies that the service type is for ICMP connections. You can optionally specify the ICMP type by name or number, between 0 and 255. For available optional ICMP type names, see the CLI help.
icmp6 [*icmp6_type*]	Specifies that the service type is for ICMP version 6 connections. You can optionally specify the ICMPv6 type by name or number, between 0 and 255. For available optional ICMPv6 type names, see the CLI help.
protocol	Identifies the protocol name or number, between 0 and 255. For a list of supported names, see the CLI help.
source *operator number*	(Optional) For **tcp**, **udp**, or **tcp-udp** protocols, specifies the source port name or number, between 0 and 65535. For a list of supported names, see the CLI help. Operators include: • **eq**—Equals the port number. • **gt**—Greater than the port number. • **lt**—Less than the port number. • **neq**—Not equal to the port number. • **range**—A range of ports. Specify two numbers separated by a space, such as **range 1024 4500**.
tcp	Specifies that the service type is for TCP connections.
tcp-udp	Specifies that the service type is for TCP or UDP connections.
udp	Specifies that the service type is for UDP connections.

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
Object-group service configuration	•	•	•	•	—

Command History

Release	Modification
8.0(1)	This command was introduced.
8.3(1)	The **object** keyword was added to support service objects (the **object service** command).

Usage Guidelines

When you create a service object group with the **object-group service** command, and you do not pre-define the protocol type for the whole group, then you can add multiple services and service objects to the group of various protocols and/or ports using the **service-object** command. When you create a service object group for a specific protocol type using the **object-group service** [**tcp** | **udp** | **tcp-udp**] command, then you can only identify the destination ports for the object group using the **port-object** command.

Examples

The following example shows how to add both TCP and UDP services to a service object group:

```
hostname(config)# object-group service CommonApps
hostname(config-service-object-group)# service-object destination tcp eq ftp
hostname(config-service-object-group)# service-object destination tcp-udp eq www
hostname(config-service-object-group)# service-object destination tcp eq h323
hostname(config-service-object-group)# service-object destination tcp eq https
hostname(config-service-object-group)# service-object destination udp eq ntp
```

The following example shows how to add multiple service objects to a service object group:

```
hostname(config)# service object SSH
hostname(config-service-object)# service tcp destination eq ssh

hostname(config)# service object EIGRP
hostname(config-service-object)# service eigrp

hostname(config)# service object HTTPS
hostname(config-service-object)# service tcp source range 0 1024 destination eq https

hostname(config)# object-group service Group1
hostname(config-service-object-group)# service-object object SSH
hostname(config-service-object-group)# service-object object EIGRP
hostname(config-service-object-group)# service-object object HTTPS
```

Related Commands

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

service-policy (class)

To apply a hierarchical policy map under another policy map, use the **service-policy** command in class configuration mode. To disable the service policy, use the **no** form of this command. Hierarchical policies are supported only for QoS traffic shaping when you want to perform priority queueing on a subset of shaped traffic.

service-policy *policymap_name*

no service-policy *policymap_name*

Syntax Description

policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map that includes the **priority** command.

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
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

Hierarchical priority queueing is used on interfaces on which you enable a traffic shaping queue. A subset of the shaped traffic can be prioritized. The standard priority queue is not used (the **priority-queue** command).

For hierarchical priority-queueing, perform the following tasks using Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map** (for priority queueing)—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **priority**—Enable priority queueing for the class map. You can only include the priority command in this policy map if you want to use is hierarchically.
3. **policy-map** (for traffic shaping)—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.

   c. **service-policy**—Call the priority queueing policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.

4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

Related Commands

Command	Description
class (policy-map)	Identifies a class map for a policy map.
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
policy-map	Identifies actions to perform on class maps.
priority	Enables priority queueing.
service-policy (global)	Applies a policy map to an interface.
shape	Enables traffic shaping.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

service-policy (global)

To activate a policy map globally on all interfaces or on a targeted interface, use the **service-policy** command in global configuration mode. To disable the service policy, use the **no** form of this command. Use the **service-policy** command to enable a set of policies on an interface.

service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

no service-policy *policymap_name* [**global** | **interface** *intf*] [**fail-close**]

Syntax Description

fail-close	Generates a syslog (767001) for IPv6 traffic that is dropped by application inspections that do not support IPv6 traffic. By default, syslogs are not generated.
global	Applies the policy map to all interfaces.
interface *intf*	Applies the policy map to a specific interface.
policymap_name	Specifies the policy map name that you configured in the **policy-map** command. You can only specify a Layer 3/4 policy map, and not an inspection policy map (**policy-map type inspect**).

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.
9.0(1)	We added the **fail-close** keyword.

Usage Guidelines

To enable the service policy, use the Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform priority queueing.
2. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. *commands for supported features*—For a given class map, you can configure many actions for various features, including QoS, application inspection, CSC or AIP SSM, TCP and UDP connections limits and timeout, and TCP normalization. See the CLI configuration guide for more details about the commands available for each feature.

3. **service-policy**—Assigns the policy map to an interface or globally.

Interface service policies take precedence over the global service policy for a given feature. For example, if you have a global policy with inspections, and an interface policy with TCP normalization, then both inspections and TCP normalization are applied to the interface. However, if you have a global policy with inspections, and an interface policy with inspections, then only the interface policy inspections are applied to that interface.

By default, the configuration includes a global policy that matches all default application inspection traffic and applies inspection to the traffic globally. You can only apply one global policy, so if you want to alter the global policy, you need to either edit the default policy or disable it and apply a new one.

The default service policy includes the following command:

```
service-policy global_policy global
```

Examples

The following example shows how to enable the inbound_policy policy map on the outside interface:

```
hostname(config)# service-policy inbound_policy interface outside
```

The following commands disable the default global policy, and enables a new one called new_global_policy on all other ASA interfaces:

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

Related Commands

Command	Description
clear configure service-policy	Clears service policy configurations.
clear service-policy	Clears service policy statistics.
service-policy (class)	Applies a hierarchical policy under another policy map.
show running-config service-policy	Displays the service policies configured in the running configuration.
show service-policy	Displays the service policy statistics.

session

To establish a Telnet session from the ASA to a module, such as an IPS SSP or a CSC SSM, to access the module CLI, use the **session** command in privileged EXEC mode.

session *id*

Syntax Description

id	Specifies the module ID: • Physical module—**1** (for slot number 1) • Software module, IPS—**ips** • Software module, ASA CX—**cxsc**

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
7.0(1)	This command was introduced.
8.6(1)	Added the **ips** module ID for the IPS SSP software module.
9.1(1)	Support for the ASA CX module was added (the **cxsc** keyword).

Usage Guidelines

This command is only available when the module is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6,** then the **x** key.

Note This command is not available for the ASA CX hardware module; it is only available for the ASA CX software module.

Examples

The following example sessions to a module in slot 1:

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Related Commands

Command	Description
debug session-command	Shows debugging messages for sessions.

session console

To establish a virtual console session from the ASA to a software module, such as an IPS SSP software module, use the **session console** command in privileged EXEC mode. This command might be useful if you cannot establish a Telnet session using the **session** command because the control plane is down.

session *id* **console**

Syntax Description

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

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)	Support for the ASA CX module was added (the **cxsc** keyword).

Usage Guidelines

To end a session, enter **Ctrl-Shift-6,** then the **x** key.

Do not use this command in conjunction with a terminal server where **Ctrl-Shift-6, x** is the escape sequence to return to the terminal server prompt. **Ctrl-Shift-6, x** is also the sequence to escape the module console and return to the ASA prompt. Therefore, if you try to exit the module console in this situation, you instead exit all the way to the terminal server prompt. If you reconnect the terminal server to the ASA, the module console session is still active; you can never exit to the ASA prompt. You must use a direct serial connection to return the console to the ASA prompt.

Use the **session** command instead.

Examples

The following example creates a console session to the IPS module:

```
hostname# session ips console

Establishing console session with slot 1
Opening console session with module ips.
Connected to module ips. Escape character sequence is 'CTRL-SHIFT-6 then x'.

sensor login: service
Password: test
```

Related Commands

Command	Description
session	Initiates a Telnet session to a module.
show module log console	Displays console log information.

session do

To establish a Telnet session and perform a command from the ASA to a module, such as an IPS SSP or a CSC SSM, use the **session do** command in privileged EXEC mode.

session *id* **do** *command*

Syntax Description

id	Specifies the module ID: • Physical module—**1** (for slot number 1) • Software module, IPS—**ips**
command	Performs a command on the module. Supported commands include: • **setup host ip** *ip_address***/***mask***,***gateway_ip*—Sets the management IP address and gateway. • **get-config**—Gets the module configuration. • **password-reset**—Resets the module password to the default.

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
7.1(1)	This command was introduced.
8.6(1)	Added the **ips** module ID for the IPS SSP software module.
8.4(4.1)	We added support for the ASA CX module.

Usage Guidelines

This command is only available when the module is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6,** then the **X** key.

Examples

The following example sets the management IP address to 10.1.1.2/24, with a default gateway of 10.1.1.1:

```
hostname# session 1 do setup host ip 10.1.1.2/24,10.1.1.1
```

Related Commands

Command	Description
debug session-command	Shows debugging messages for sessions.

session ip

To configure logging IP addresses for the module, such as an IPS SSP or a CSC SSM, use the **session ip** command in privileged EXEC mode.

session *id* **ip** {**address** *address mask* | **gateway** *address*}

Syntax Description

id	Specifies the module ID: • Physical module—**1** (for slot number 1) • Software module, IPS—**ips**
address *address*	Sets the syslog server address.
gateway *address*	Sets the gateway to the syslog server.
mask	Sets the subnet 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
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.1(1)	This command was introduced.
8.4(4.1)	We added support for the ASA CX module.
8.6(1)	Added the **ips** module ID for the IPS SSP software module.

Usage Guidelines

This command is only available when the module is in the Up state. See the **show module** command for state information.

To end a session, enter **exit** or **Ctrl-Shift-6,** then the **X** key.

Examples

The following example sessions to a module in slot 1:

```
hostname# session 1 ip address
```

Related Commands

Command	Description
debug session-command	Shows debugging messages for sessions.

set connection

To specify connection limits within a policy map for a traffic class, use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

Syntax Description

conn-max *n*	Sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 2000000. The default is 0, which allows unlimited connections. For example, if two servers are configured to allow simultaneous TCP and/or UDP connections, the connection limit is applied to each configured server separately. When configured under a class, this argument restricts the maximum number of simultaneous connections that are allowed for the entire class. In this case, one attack host can consume all the connections and leave none of the rest of the hosts matched in the access list under the class.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic connections allowed, between 0 and 2000000. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 2000000. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the ASA. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	Sets the maximum number of simultaneous connections allowed per client, between 0 and 2000000. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the ASA. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for each host that is matched through an access list under the class.
random-sequence-number {**enable** | **disable**}	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.

Defaults

For the **conn-max**, **embryonic-conn-max**, **per-client-embryonic-max**, and **per-client-max** parameters, the default value of *n* is 0, which allows unlimited connections.

Sequence number randomization 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
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	The **per-client-embryonic-max** and **per-client-max** keywords were added.
8.0(2)	This command is now available for a Layer 3/4 management class map, for to-the-ASA management traffic. Only the **conn-max** and **embryonic-conn-max** keywords are available.
9.0(1)	The maximum number of connections was increased from 65535 to 2000000.

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command (for through traffic) or **class-map type management** command (for management traffic). Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the CLI configuration guide.

Note Depending on the number of CPU cores on your ASA model, the maximum concurrent and embryonic connections may exceed the configured numbers due to the way each core manages connections. In the worst case scenario, the ASA allows up to *n*-1 extra connections and embryonic connections, where *n* is the number of cores. For example, if your model has 4 cores, if you configure 6 concurrent connections and 4 embryonic connections, you could have an additional 3 of each type. To determine the number of cores for your model, enter the **show cpu core** command.

TCP Intercept Overview

Limiting the number of embryonic connections protects you from a DoS attack. The ASA uses the per-client limits and the embryonic connection 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. TCP Intercept uses the SYN cookies algorithm to prevent TCP SYN-flooding attacks. A SYN-flooding attack consists of a series of SYN packets usually originating from spoofed IP addresses. The constant flood of SYN packets keeps the server SYN queue full, which prevents it from servicing connection requests. When the embryonic connection threshold of a connection is crossed, the ASA acts as a proxy for the server and generates a SYN-ACK response to the client SYN request. When the ASA receives an ACK back from the client, it can then authenticate the client and allow the connection to the server.

Disabling TCP Intercept for Management Packets for Clientless SSL Compatibility

By default, TCP management connections have TCP Intercept always enabled. When TCP Intercept is enabled, it intercepts the 3-way TCP connection establishment handshake packets and thus deprives the ASA from processing the packets for clientless SSL. Clientless SSL requires the ability to process the 3-way handshake packets to provide selective ACK and other TCP options for clientless SSL connections. To disable TCP Intercept for management traffic, you can set the embryonic connection limit; only after the embryonic connection limit is reached is TCP Intercept enabled.

TCP Sequence Randomization Overview

Each TCP connection has two ISNs: one generated by the client and one generated by the server. The ASA 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 ASA, and the eBGP peers are using MD5. Randomization breaks the MD5 checksum.
- You use a WAAS device that requires the ASA not to randomize the sequence numbers of connections.

Examples

The following is an example of the use of the **set connection** command configure the maximum number of simultaneous connections as 256 and to disable TCP sequence number randomization:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
hostname(config-pmap-c)#
```

The following is an example of the use of the **set connection** command in a service policy that diverts traffic to a CSC SSM. The **set connection** command restricts each client whose traffic the CSC SSM scans to a maximum of five connections.

```
hostname(config)# policy-map csc_policy
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection per-client-max 5
hostname(config-pmap-c)# csc fail-close
hostname(config-pmap-c)#
```

You can enter this command with multiple parameters or you can enter each parameter as a separate command. The ASA combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

the output of the **show running-config policy-map** command would display the result of the two commands in a single, combined command:

```
set connection conn-max 600 embryonic-conn-max 50
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Removes all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy-map configurations.
show service-policy	Displays service policy configuration. Use the **set connection** keyword to view policies that include the **set connection** command.

set connection advanced-options

To customize TCP normalization, use the **set connection advanced-options** command in class configuration mode. To remove the TCP normalization options, use the **no** form of this command.

set connection advanced-options *tcp_mapname*

no set connection advanced-options *tcp_mapname*

Syntax Description

tcp_mapname	Name of a TCP map created by the **tcp-map** command.

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
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To enable TCP state bypass, use the Modular Policy Framework:

1. **tcp-map**—Identify the TCP normalization actions.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization actions.
3. **policy-map**—Identify the actions associated with the class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced options**—Apply TCP normalization to the class map.
4. **service-policy**—Assigns the policy map to an interface or globally.

Examples

The following example shows the use of the **set connection advanced-options** command to specify the use of a TCP map named localmap:

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit
hostname(config)# tcp-map localmap
hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
class-map	Configures a traffic class by issuing at most one (with the exception of tunnel-group and default-inspection-traffic) match command, specifying match criteria, in the class-map configuration mode.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Display all current policy-map configurations.

set connection advanced-options tcp-state-bypass

To enable TCP state bypass, use the **set connection advanced-options** command in class configuration mode. The class configuration mode is accessible from the policy-map configuration mode. To disable TCP state bypass, use the **no** form of this command.

set connection advanced-options tcp-state-bypass

no set connection advanced-options tcp-state-bypass

Syntax Description

This command has no arguments or keywords.

Defaults

By default, TCP state bypass 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**
Class configuration	•	•	•	•	—

Command History

Release	Modification
8.2(1)	This command was introduced.

Usage Guidelines

To enable TCP state bypass, use the Modular Policy Framework:

1. **class-map**—Identify the traffic on which you want to perform TCP state bypass.
2. **policy-map**—Identify the actions associated with the class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced options tcp-state-bypass**—Apply traffic shaping to the class map.
3. **service-policy**—Assigns the policy map to an interface or globally.

Allowing Outbound and Inbound Flows through Separate Devices

By default, all traffic that goes through the ASA is inspected using the Adaptive Security Algorithm and is either allowed through or dropped based on the security policy. The ASA maximizes the firewall performance by checking the state of each packet (is this a new connection or an established connection?) and assigning it to either the session management path (a new connection SYN packet), the fast path (an established connection), or the control plane path (advanced inspection).

TCP packets that match existing connections in the fast path can pass through the ASA without rechecking every aspect of the security policy. This feature maximizes performance. However, the method of establishing the session in the fast path using the SYN packet, and the checks that occur in the fast path (such as TCP sequence number), can stand in the way of asymmetrical routing solutions: both the outbound and inbound flow of a connection must pass through the same ASA.

For example, a new connection goes to ASA 1. The SYN packet goes through the session management path, and an entry for the connection is added to the fast path table. If subsequent packets of this connection go through ASA 1, then the packets will match the entry in the fast path, and are passed through. But if subsequent packets go to ASA 2, where there was not a SYN packet that went through the session management path, then there is no entry in the fast path for the connection, and the packets are dropped.

If you have asymmetric routing configured on upstream routers, and traffic alternates between two ASAs, then you can configure TCP state bypass for specific traffic. TCP state bypass alters the way sessions are established in the fast path and disables the fast path checks. This feature treats TCP traffic much as it treats a UDP connection: when a non-SYN packet matching the specified networks enters the ASA, and there is not a fast path entry, then the packet goes through the session management path to establish the connection in the fast path. Once in the fast path, the traffic bypasses the fast path checks.

Unsupported Features

The following features are not supported when you use TCP state bypass:

- Application inspection—Application inspection requires both inbound and outbound traffic to go through the same ASA, so application inspection is not supported with TCP state bypass.
- AAA authenticated sessions—When a user authenticates with one ASA, traffic returning via the other ASA will be denied because the user did not authenticate with that ASA.
- TCP Intercept, maximum embryonic connection limit, TCP sequence number randomization—The ASA does not keep track of the state of the connection, so these features are not applied.
- TCP normalization—The TCP normalizer is disabled.
- SSM functionality—You cannot use TCP state bypass and any application running on an SSM, such as IPS or CSC.

NAT Guidelines

Because the translation session is established separately for each ASA, be sure to configure static NAT on both ASAs for TCP state bypass traffic; if you use dynamic NAT, the address chosen for the session on ASA 1 will differ from the address chosen for the session on ASA 2.

Connection Timeout Guidelines

If there is no traffic on a given connection for 2 minutes, the connection times out. You can override this default using the **set connection timeout tcp** command. Normal TCP connections timeout by default after 60 minutes.

Examples

The following is an example configuration for TCP state bypass:

```
hostname(config)# access-list tcp_bypass extended permit tcp 10.1.1.0 255.255.255.224 any

hostname(config)# class-map tcp_bypass
hostname(config-cmap)# description "TCP traffic that bypasses stateful firewall"
hostname(config-cmap)# match access-list tcp_bypass

hostname(config-cmap)# policy-map tcp_bypass_policy
hostname(config-pmap)# class tcp_bypass
hostname(config-pmap-c)# set connection advanced-options tcp-state-bypass

hostname(config-pmap-c)# service-policy tcp_bypass_policy outside

hostname(config-pmap-c)# static (inside,outside) 209.165.200.224 10.1.1.0 netmask
255.255.255.224
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
set connection timeout	Sets the connection timeouts.

set connection decrement-ttl

To decrement the time to live value within a policy map for a traffic class, use the **set connection decrement-ttl** command in class configuration mode. To not decrement the time to live, use the **no** form of this command.

set connection decrement-ttl

no set connection decrement-ttl

Syntax Description

This command has no arguments or keywords.

Defaults

By default, the ASA does not decrement the time to live.

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
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.2(2)	This command was introduced.

Usage Guidelines

This command, along with the **icmp unreachable** command, is required to allow a traceroute through the ASA that shows the ASA as one of the hops.

Examples

The following example enables time to live decrements and sets the ICMP unreachable rate limit:

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp unreachable rate-limit 50 burst-size 6
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
clear configure policy-map	Removes all policy map configuration, except if a policy map is in use in a **service-policy** command, that policy map is not removed.
icmp unreachable	Controls the rate at which ICMP unreachables are allowed through the ASA.

policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current policy map configurations.
show service-policy	Displays service policy configuration.

set connection timeout

To specify connection timeouts within a policy map for a traffic class, use the **set connection timeout** command in class configuration mode. To remove the timeout, use the **no** form of this command.

set connection timeout {[**embryonic** *hh***:***mm***:***ss*] [**idle** *hh***:***mm***:***ss* [**reset**]] [**half-closed** *hh***:***mm***:***ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

no set connection timeout {[**embryonic** *hh***:***mm***:***ss*] [**idle** *hh***:***mm***:***ss* [**reset**]] [**half-closed** *hh***:***mm***:***ss*] [**dcd** [*retry_interval* [*max_retries*]]]}

Syntax Description

dcd	Enables dead connection detection (DCD). DCD detects a dead connection and allows it to expire, without expiring connections that can still handle traffic. You configure DCD when you want idle, but valid connections to persist. After a TCP connection times out, the ASA sends DCD probes to the end hosts to determine the validity of the connection. If one of the end hosts fails to respond after the maximum retries are exhausted, the ASA frees the connection. If both end hosts respond that the connection is valid, the ASA updates the activity timeout to the current time and reschedules the idle timeout accordingly.
embryonic *hh***:***mm***:***ss*	Sets the timeout period until a TCP embryonic (half-open) connection is closed, between 0:0:5 and 1193:0:0. The default is 0:0:30. You can also set the value to 0, which means the connection never times out. A TCP connection for which a three-way handshake is not complete is an embryonic connection.
half-closed *hh***:***mm***:***ss*	Sets the idle timeout period until a half-closed connection is closed, between 0:5:0 (for 9.1(1) and earlier) or 0:0:30 (for 9.1(2) and later) and 1193:0:0. The default is 0:10:0. You can also set the value to 0, which means the connection never times out. Half-closed connections are not affected by DCD. Also, the ASA does not send a reset when taking down half-closed connections.
idle *hh***:***mm***:***ss*	Sets the idle timeout period after which an established connection of any protocol closes. The valid range is from 0:0:1 to 1193:0:0.
max_retries	Sets the number of consecutive failed retries for DCD before declaring the connection as dead. The minimum value is 1 and the maximum value is 255. The default is 5.
reset	For TCP traffic only, sends a TCP RST packet to both end systems after idle connections are removed.
retry_interval	Time duration in *hh***:***mm***:***ss* format to wait after each unresponsive DCD probe before sending another probe, between 0:0:1 and 24:0:0. The default is 0:0:15.

Defaults

The default **embryonic** timeout is 30 seconds.

The default **half-closed** idle timeout is 10 minutes.

The default **dcd** *max_retries* value is 5.

The default **dcd** *retry_interval* value is 15 seconds.

The default **tcp** idle timeout is 1 hour.

The default **udp** idle timeout is 2 minutes.

The default **icmp** idle timeout is 2 seconds.

The default **esp** and **ha** idle timeout is 30 seconds.

For all other protocols, the default idle timeout is 2 minutes.

To never time out, enter 0:0:0.

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**
Class configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(1)	Support for DCD was added.
8.2(2)	The **tcp** keyword was deprecated in favor of the **idle** keyword, which controls the idle timeout for all protocols.
9.1(2)	The minimum **half-closed** value was lowered to 30 seconds (0:0:30).

Usage Guidelines

Configure this command using Modular Policy Framework. First define the traffic to which you want to apply the timeout using the **class-map** command. Then enter the **policy-map** command to define the policy, and enter the **class** command to reference the class map. In class configuration mode, you can enter the **set connection timeout** command. Finally, apply the policy map to an interface using the **service-policy** command. For more information about how Modular Policy Framework works, see the CLI configuration guide.

Enabling DCD changes the behavior of idle-timeout handling in the TCP normalizer. DCD probing resets the idle timeout on the connections that appear in the **show conn** command. To determine when a connection that has exceeded the configured timeout value in the timeout command but has been kept alive due to DCD probing, use the **show service-policy** command to include counters to show the amount of activity from DCD.

Examples

The following example sets the connection timeouts for all traffic:

```
hostname(config)# class-map CONNS
hostname(config-cmap)# match any
hostname(config-cmap)# policy-map CONNS
hostname(config-pmap)# class CONNS
hostname(config-pmap-c)# set connection timeout idle 2:0:0 embryonic 0:40:0 half-closed
0:20:0 dcd
hostname(config-pmap-c)# service-policy CONNS interface outside
```

You can enter **set connection** commands with multiple parameters, or you can enter each parameter as a separate command. The ASA combines the commands into one line in the running configuration. For example, if you entered the following two commands in class configuration mode:

```
hostname(config-pmap-c)# set connection timeout idle 2:0:0
hostname(config-pmap-c)# set connection timeout embryonic 0:40:0
```

Then the output of the **show running-config policy-map** command would display the result of the two commands in the following single, combined command:

```
set connection timeout tcp 2:0:0 embryonic 0:40:0
```

Related Commands

Command	Description
class	Specifies a class-map to use for traffic classification.
clear configure policy-map	Remove all policy-map configuration, except that if a policy-map is in use in a service-policy command, that policy-map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configure connection values.
show running-config policy-map	Display all current policy-map configurations.
show service-policy	Displays counters for DCD `and` other service activity.

set metric

To set the metric value of a route for OSPF and other dynamic routing protocols in a route map, use the **set metric** command in route-map configuration mode. To return to the default metric value for OSPF and other dynamic routing protocols, use the **no** form of this command.

set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

no set metric *metric-value* | [*bandwidth delay reliability loading mtu*]

Syntax Description

bandwidth	EIGRP bandwidth of a route, in kbps. Valid values range from 0 to 4294967295.
delay	EIGRP route delay, in tens of microseconds. Valid values range from 0 to 4294967295.
loading	Effective EIGRP bandwidth of a route expressed as a number from 0 to 255. The value 255 means 100 percent loading.
metric-value	Metric value of a route for OSPF and other dynamic routing protocols (except for EIGRP), expressed as a number. Valid values range from 0 to 4294967295.
mtu	Minimum MTU size of a route for EIGRP, in bytes. Valid values range from 0 to 4294967295.
reliability	Likelihood of successful packet transmission for EIGRP expressed as a number from 0 to 255. The value 255 means 100 percent reliability; 0 means no reliability.

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**
Route-map configuration	•	—	•	•	—

Command History

Release	**Modification**
7.0(1)	This command was introduced.
8.2(5)	Added the *bandwidth*, *delay*, *reliability*, *loading*, and *mtu* arguments to support EIGRP in a route map.
9.0(1)	Multiple context mode is supported.

Usage Guidelines

The **no set metric** command allows you to return to the default metric value for OSPF and other dynamic routing protocols. In this context, the *metric-value* argument is an integer from 0 to 4294967295.

Examples

The following example shows how to configure a route map for OSPF routing:

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
```

The following example shows how to set the metric value for EIGRP in a route map:

```
hostname(config)# access-list route-out line 1 standard permit 10.1.1.0 255.255.255.0
hostname(config)# route-map rmap permit 10
hostname(config-route-map)# set metric 10000 60 100 1 1500
hostname(config-route-map)# show route-map rmap
route-map rmap, permit, sequence 10
  Match clauses:
    ip address (access-lists): route-out
  Set clauses:
    metric 10000 60 100 1 1500
hostname(config-route-map)# show running-config route-map
route-map rmap permit 10
 match ip address route-out
 set metric 10000 60 100 1 1500
```

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out of one of the interfaces specified,
match ip next-hop	Distributes any routes that have a next-hop router address that is passed by one of the access lists specified.
route-map	Defines the conditions for redistributing routes from one routing protocol into another.

set metric-type

To specify the type of OSPF metric routes, use the **set metric-type** command in route-map configuration mode. To return to the default setting, use the **no** form of this command.

set metric-type {**type-1** | **type-2**}

no set metric-type

Syntax Description

type-1	Specifies the type of OSPF metric routes that are external to a specified autonomous system.
type-2	Specifies the type of OSPF metric routes that are external to a specified autonomous system.

Defaults

The default is **type-2**.

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
Route-map configuration	•	—	•	•	—

Command History

Release	Modification
7.0(1)	This command was introduced.
9.0(1)	Multiple context mode is supported.

Examples

The following example shows how to configure a route map for OSPF routing:

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

Related Commands

Command	Description
match interface	Distributes any routes that have their next hop out one of the interfaces specified,
route-map	Defines the conditions for redistributing routes from one routing protocol into another.
set metric	Specifies the metric value in the destination routing protocol for a route map.

setup

To configure a minimal configuration for the ASA using interactive prompts, enter the **setup** command in global configuration mode.

setup

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.
8.4(1)	In routed mode for the ASA 5510 and higher, the interface configured is now the Management *slot/port* interface, and not the "inside" interface. For the ASA 5505, the interface configured is the VLAN 1 interface, not "inside".
9.0(1)	The default configuration prompt was changed, and Ctrl + Z to exit the setup process was enabled.

Usage Guidelines

The setup prompt automatically appears at boot time if there is no startup configuration in flash memory.

The **setup** command walks you through minimal configuration to establish ASDM connectivity. This command is designed for a unit that has either no configuration or a partial configuration. If your model supports a factory default configuration, we recommend using the factory default configuration instead of the **setup** command (to restore the default configuration, use the **configure factory-default** command).

The **setup** command requires an already-named interface called "management".

When you enter the **setup** command, you are asked for the information in Table 43-1. If there is already a configuration for the listed parameter, it appears in brackets, so you can either accept it as the default or override it by entering a new value. The exact prompts available may differ per model. The system **setup** command includes a subset of these prompts.

Table 43-1 Setup Prompts

Prompt	Description
`Pre-configure Firewall now through interactive prompts [yes]?`	Enter **yes** or **no**. If you enter **yes**, the setup continues. If **no**, the setup stops and the global configuration prompt (hostname(config)#) appears.
`Firewall Mode [Routed]:`	Enter **routed** or **transparent**.
`Enable password:`	Enter an enable password. (The password must have at least three characters.)
`Allow password recovery [yes]?`	Enter **yes** or **no**.
`Clock (UTC):`	You cannot enter anything in this field. The UTC time is used by default.
`Year:`	Enter the year using four digits, for example, 2005. The year range is 1993 to 2035.
`Month:`	Enter the month using the first three characters of its name, for example, **Sep** for September.
`Day:`	Enter the day of the month, from 1 to 31.
`Time:`	Enter the hour, minutes, and seconds in 24-hour time format, for example, enter **20:54:44** for 8:54 p.m and 44 seconds.
`Host name:`	Enter the hostname that you want to display in the command line prompt.
`Domain name:`	Enter the domain name of the network on which the ASA runs.
`IP address of host running Device Manager:`	Enter the IP address of the host that needs to access ASDM.
`Use this configuration and save to flash (yes)?`	Enter **yes** or **no**. If you enter **yes**, the inside interface is enabled and the requested configuration is written to the Flash partition. If you enter **no**, the setup prompt repeats, beginning with the first question: `Pre-configure Firewall now through interactive prompts [yes]?` Enter **Ctrl + Z** to exit the setup or **yes** to repeat the prompt.

Examples

The following example shows how to complete the **setup** command:

```
hostname(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
```

```
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: example.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

Related Commands

Command	Description
configure factory-default	Restores the default configuration.

shape

To enable QoS traffic shaping, use the **shape** command in class configuration mode. If you have a device that transmits packets at a high speed, such as a ASA with Fast Ethernet, and it is connected to a low speed device such as a cable modem, then the cable modem is a bottleneck at which packets are frequently dropped. To manage networks with differing line speeds, you can configure the ASA to transmit packets at a fixed slower rate, called *traffic shaping*. To remove this configuration, use the **no** form of this command.

Note Traffic shaping is only supported on the ASA 5505, 5510, 5520, 5540, and 5550. Multi-core models (such as the ASA 5500-X) do not support shaping.

shape average *rate* [*burst_size*]

no shape average *rate* [*burst_size*]

Syntax Description

average *rate*	Sets the average rate of traffic in bits per second over a given fixed time period, between 64000 and 154400000. Specify a value that is a multiple of 8000. See the "Usage Guidelines" section for more information about how the time period is calculated.
burst_size	Sets the average burst size in bits that can be transmitted over a given fixed time period, between 2048 and 154400000. Specify a value that is a multiple of 128. If you do not specify the *burst_size*, the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

Defaults

If you do not specify the *burst_size*, the default value is equivalent to 4-milliseconds of traffic at the specified average rate. For example, if the average rate is 1000000 bits per second, 4 ms worth = 1000000 * 4/1000 = 4000.

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
Class configuration	•	•	•	—	—

Command History

Release	Modification
7.2(4)/8.0(4)	This command was introduced.

Usage Guidelines

To enable traffic shaping, use the Modular Policy Framework:

1. **policy-map**—Identify the actions associated with the **class-default** class map.
   a. **class class-default**—Identify the **class-default** class map on which you want to perform actions.
   b. **shape**—Apply traffic shaping to the class map.
   c. (Optional) **service-policy**—Call a different policy map in which you configured the **priority** command so you can apply priority queueing to a subset of shaped traffic.
2. **service-policy**—Assigns the policy map to an interface or globally.

Traffic Shaping Overview

Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

- Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic.
- Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to be transmitted, including all the possible overhead such as the IPsec header and L2 header.
- The shaped traffic includes both through-the-box and from-the-box traffic.
- The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the burst size value. See the CLI configuration guide for more information about the token bucket.
- When bursty traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queueing, see the **priority** command):
  - The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200-milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.
  - When the queue limit is reached, packets are tail-dropped.
  - Certain critical keep-alive packets such as OSPF Hello packets are never dropped.
  - The time interval is derived by *time_interval* = *burst_size* / *average_rate*. The larger the time interval is, the burstier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

    Average Rate = 1000000

    Burst Size = 1000000

    In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay-sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

How QoS Features Interact

You can configure each of the QoS features alone if desired for the ASA. Often, though, you configure multiple QoS features on the ASA so you can prioritize some traffic, for example, and prevent other traffic from causing bandwidth problems.

See the following supported feature combinations per interface:

- Standard priority queuing (for specific traffic) + Policing (for the rest of the traffic).

  You cannot configure priority queueing and policing for the same set of traffic.
- Traffic shaping (for all traffic on an interface) + Hierarchical priority queueing (for a subset of traffic).

You cannot configure traffic shaping and standard priority queueing for the same interface; only hierarchical priority queueing is allowed. For example, if you configure standard priority queueing for the global policy, and then configure traffic shaping for a specific interface, the feature you configured last is rejected because the global policy overlaps the interface policy.

Typically, if you enable traffic shaping, you do not also enable policing for the same traffic, although the ASA does not restrict you from configuring this.

Examples

The following example enables traffic shaping for all traffic on the outside interface, and prioritizes traffic within VPN tunnel-grp1 with the DSCP bit set to ef:

```
hostname(config)# class-map TG1-voice
hostname(config-cmap)# match tunnel-group tunnel-grp1
hostname(config-cmap)# match dscp ef

hostname(config)# policy-map priority-sub-policy
hostname(config-pmap)# class TG1-voice
hostname(config-pmap-c)# priority

hostname(config-pmap-c)# policy-map shape_policy
hostname(config-pmap)# class class-default
hostname(config-pmap-c)# shape
hostname(config-pmap-c)# service-policy priority-sub-policy

hostname(config-pmap-c)# service-policy shape_policy interface outside
```

Related Commands

Command	Description
class	Identifies the class map on which you want to perform actions in a policy map.
police	Enables QoS policing.
policy-map	Identifies actions to apply to traffic in a service policy.
priority	Enables QoS priority queueing.
service-policy (class)	Applies a hierarchical policy map.
service-policy (global)	Applies a service policy to interface(s).
show service-policy	Shows QoS statistics.