CHAPTER 12

eigrp log-neighbor-changes through functions (removed) Commands

eigrp log-neighbor-changes

To enable the logging of EIGRP neighbor adjacency changes, use the **eigrp log-neighbor-changes** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Defaults

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **eigrp log-neighbor-changes** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor changes:

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-changes
```

Related Commands

Command	Description
eigrp log-neighbor-warnings	Enables logging of neighbor warning messages.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp log-neighbor-warnings

To enable the logging of EIGRP neighbor warning messages, use the **eigrp log-neighbor-warnings** command in router configuration mode. To turn off this function, use the **no** form of this command.

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

Syntax Description

seconds	(Optional) The time interval (in seconds) between repeated neighbor warning messages. Valid values are from 1 to 65535. Repeated warnings are not logged if they occur during this interval.

Defaults

This command is enabled by default. All neighbor warning messages are logged.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **eigrp log-neighbor-warnings** command is enabled by default; only the **no** form of the command appears in the running configuration.

Examples

The following example disables the logging of EIGRP neighbor warning messages:

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-warnings
```

The following example logs EIGRP neighbor warning messages and repeats the warning messages in 5-minute (300 seconds) intervals:

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp log-neighbor-warnings 300
```

Related Commands

Command	Description
eigrp log-neighbor-messages	Enables the logging of changes in EIGRP neighbor adjacencies.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp router-id

To specify router ID used by the EIGRP routing process, use the **eigrp router-id** command in router configuration mode. To restore the default value, use the **no** form of this command.

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

Syntax Description

ip-addr	Router ID in IP address (dotted-decimal) format. You cannot use 0.0.0.0 or 255.255.255.255 as the router ID.

Defaults

If not specified, the highest-level IP address on the security appliance is used as the router ID.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

If the **eigrp router-id** command is not configured, EIGRP automatically selects the highest IP address on the security appliance to use as the router ID when an EIGRP process is started.The router ID is not changed unless the EIGRP process is removed using the **no router eigrp** command or unless the router ID is manually configured with the **eigrp router-id** command.

The router ID is used to identify the originating router for external routes. If an external route is received with the local router ID, the route is discarded. To prevent this, use the **eigrp router-id** command to specify a global address for the router ID.

A unique value should be configured for each EIGRP router.

Examples

The following example configures 172.16.1.3 as a fixed router ID for the EIGRP routing process:

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp router-id 172.16.1.3
```

Related Commands

Command	Description
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

eigrp stub

To configure the EIGRP routing process as a stub routing process, use the **eigrp stub** command in router configuration mode. To remove EIGRP stub routing, use the **no** form of this command.

eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [receive-only] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

Syntax Description

connected	(Optional) Advertises connected routes.
receive-only	(Optional) Sets the security appliance as a received-only neighbor.
redistributed	(Optional) Advertises routes redistributed from other routing protocols.
static	(Optional) Advertises static routes.
summary	(Optional) Advertises summary routes.

Defaults

Stub routing is not 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**
Router configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **eigrp stub** command to configure the security appliance as a stub where the security appliance directs all IP traffic to a distribution router.

Using the **receive-only** keyword restricts the security appliance from sharing any of its routes with any other router in the autonomous system; the security appliance only receives updates from the EIGRP neighbor. You cannot use any other keyword with the **receive-only** keyword.

You can specify one or more of the **connected**, **static**, **summary**, and **redistributed** keywords. If any of these keywords is used with the **eigrp stub** command, only the route types specified by the particular keyword are sent.

The **connected** keyword permits the EIGRP stub routing process to send connected routes. If the connected routes are not covered by a **network** statement, it may be necessary to redistribute connected routes with the **redistribute** command under the EIGRP process.

The **static** keyword permits the EIGRP stub routing process to send static routes. Without the configuration of this option, EIGRP will not send any static routes. If the static routes are not covered by a **network** statement, it may be necessary to redistribute them with the **redistribute** command under the EIGRP process.

The **summary** keyword permits the EIGRP stub routing process to send summary routes. You can create summary routes manually with the **summary-address eigrp** command or automatically with the **auto-summary** command enabled (**auto-summary** is enabled by default).

The **redistributed** keyword permits the EIGRP stub routing process to send routes redistributed into the EIGRP routing process from other routing protocols. If you do you configure this option, EIGRP does not advertise redistributed routes.

Examples

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that advertises connected and summary routes:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected summary
```

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that advertises connected and static routes. Sending summary routes is not permitted.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected static
```

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that only receives EIGRP updates. Connected, summary, and static route information is not sent.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 eigrp
hostname(config-router)# eigrp stub receive-only
```

The following example uses the **eigrp stub** command to configure the security appliance as an EIGRP stub that advertises routes redistributed into EIGRP from other routing protocols:

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub redistributed
```

The following example uses the **eigrp stub** command without any of the optional arguments. When used without arugments, the **eigrp stub** commands advertises connected and static routes by default.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub
```

Related Commands

Command	Description
router eigrp	Clears the EIGRP router configuration mode commands from the running configuration.
show running-config router eigrp	Displays the EIGRP router configuration mode commands in the running configuration.

eject

To support the removal of an ASA 5500 series external compact Flash device, use the **eject** command in user EXEC mode.

eject [*/noconfirm*] *disk1:*

Syntax Description

disk1:	Specifies the device to eject.
/noconfirm	Specifies that you do not need to confirm device removal before physically removing the external Flash device from the security appliance.

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
User EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The **eject** command allows you to safely remove a compact Flash device from an ASA 5500 series security appliance.

The following example shows how to use the **eject** command to shut down *disk1* gracefully before the device is physically removed from the security appliance:

```
hostname# eject /noconfig disk1:
It is now safe to remove disk1:
hostname# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

Related Commands

Command	Description
show version	Displays information about the operating system software.

email

To include the indicated email address in the Subject Alternative Name extension of the certificate during enrollment, use the **email** command in crypto ca-trustpoint configuration mode. To restore the default setting, use the **no** form of this command.

email *address*

no email

Syntax Description

address	Specifies the email address. The maximum length of *address* is 64 characters.

Defaults

The default setting is not set.

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	This command was introduced.

Examples

The following example enters crypto ca-trustpoint configuration mode for trustpoint central, and includes the email address user1@user.net in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca-trustpoint central
hostname(ca-trustpoint)# email user1@user.net
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca-trustpoint	Enters trustpoint configuration mode.

enable

To enter privileged EXEC mode, use the **enable** command in user EXEC mode.

enable [*level*]

Syntax Description

level	(Optional) The privilege level between 0 and 15. Not used with enable authentication (the **aaa authentication enable console** command).

Defaults

Enters privilege level 15 unless you are using enable authentication (using the **aaa authentication enable console** command), in which case the default level depends on the level configured for your username.

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
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The default enable password is blank. See the **enable password** command to set the password.

Without enable authentication, when you enter the **enable** command, your username changes to enable_*level*, where the default level is 15. With enable authentication (using the **aaa authentication enable console** command), the username and associated level are preserved. Preserving the username is important for command authorization (the **aaa authorization command** command, using either local or TACACS+).

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode. To use levels in between, enable local command authorization (the **aaa authorization command LOCAL** command) and set the commands to different privilege levels using the **privilege** command. TACACS+ command authorization does not use the privilege levels configured on the security appliance.

See the **show curpriv** command to view your current privilege level.

Enter the **disable** command to exit privileged EXEC mode.

Examples

The following example enters privileged EXEC mode:

```
hostname> enable
Password: Pa$$w0rd
hostname#
```

The following example enters privileged EXEC mode for level 10:

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

Related Commands

Command	Description
enable password	Sets the enable password.
disable	Exits privileged EXEC mode.
aaa authorization command	Configures command authorization.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.

enable (webvpn)

To enable WebVPN or e-mail proxy access on a previously configured interface, use the enable command. For WebVPN, use this command in webvpn mode. For e-mail proxies (IMAP4S. POP3S, SMTPS), use this command in the applicable e-mail proxy mode. To disable WebVPN on an interface, use the **no** version of the command.

enable *ifname*

no enable

Syntax Description

ifname	Identifies the previously configured inteface. Use the **nameif** command to configure interfaces.

Defaults

WebVPN 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
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example shows how to enable WebVPN on the interface named Outside:

```
hostname(config)# webvpn
hostname(config-webvpn)# enable Outside
```

The following example shows how to configure POP3S e-mail proxy on the interface named Outside:

```
hostname(config)# pop3s
hostname(config-pop3s)# enable Outside
```

enable gprs

To enable GPRS with RADIUS accounting, use the **enable gprs** command in radius-accounting parameter configuration mode, which is accessed by using the **inspect radius-accounting** command. The security appliance checks for the 3GPP VSA 26-10415 in the Accounting-Request Stop messages to properly handle secondary PDP contexts. To disable this command, use the **no** form of this command.

enable gprs

no enable gprs

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
radius-accounting parameter configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This option is disabled by default. A GTP license is required to enable this feature.

Examples

The following example shows how to enable GPRS with RADIUS accounting:

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enable gprs
```

Related Commands

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

enable password

To set the enable password for privileged EXEC mode, use the **enable password** command in global configuration mode. To remove the password for a level other than 15, use the **no** form of this command. You cannot remove the level 15 password.

enable password *password* **[level** *level*] [**encrypted**]

no enable password level *level*

Syntax Description

encrypted	(Optional) Specifies that the password is in encrypted form. The password is saved in the configuration in encrypted form, so you cannot view the original password after you enter it. If for some reason you need to copy the password to another security appliance but do not know the original password, you can enter the **enable password** command with the encrypted password and this keyword. Normally, you only see this keyword when you enter the **show running-config enable** command.
level *level*	(Optional) Sets a password for a privilege level between 0 and 15.
password	Sets the password as a case-sensitive string of 3 to 32 alphanumeric and special characters. You can use any character in the password except a question mark or a space.

Defaults

The default password is blank. The default level is 15.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The default password for enable level 15 (the default level) is blank. To reset the password to be blank, do not enter any text for the *password* argument.

For multiple context mode, you can create an enable password for the system configuration as well as for each context.

To use privilege levels other than the default of 15, configure local command authorization (see the **aaa authorization command** command and specify the **LOCAL** keyword), and set the commands to different privilege levels using the **privilege** command. If you do not configure local command authorization, the enable levels are ignored, and you have access to level 15 regardless of the level you set. See the **show curpriv** command to view your current privilege level.

Levels 2 and above enter privileged EXEC mode. Levels 0 and 1 enter user EXEC mode.

Examples

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

```
hostname(config)# enable password Pa$$w0rd
```

The following example sets the enable password to Pa$$w0rd10 for level 10:

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

The following example sets the enable password to an encrypted password that you copied from another security appliance:

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

Related Commands

Command	Description
aaa authorization command	Configures command authorization.
enable	Enters privileged EXEC mode.
privilege	Sets the command privilege levels for local command authorization.
show curpriv	Shows the currently logged in username and the user privilege level.
show running-config enable	Shows the enable passwords in encrypted form.

endpoint

To add an endpoint to an HSI group for H.323 protocol inspection, use the **endpoint** command in hsi group configuration mode. To disable this feature, use the **no** form of this command.

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

Syntax Description

if_name	The interface through which the endpoint is connected to the security appliance.
ip_address	IP address of the endpoint to add. A maximum of ten endpoints per HSI group is allowed.

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
HSI group configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to add endpoints to an HSI group in an H.323 inspection policy map:

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

Related Commands

Command	Description
class-map	Creates a Layer 3/4 class map.
hsi-group	Creates an HSI group.
hsi	Adds an HSI to the HSI group.
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

endpoint-mapper

To configure endpoint mapper options for DCERPC inspection, use the **endpoint-mapper** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

Syntax Description

epm-service-only	Specifies to enforce endoint mapper service during binding.
lookup-operation	Specifies to enable lookup operation of the endpoint mapper service.
timeout *value*	Specifies the timeout for pinholes from the lookup operation. Range is from 0:0:1 to 1193:0:0.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to configure the endpoint mapper in a DCERPC policy map:

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# endpoint-mapper epm-service-only
```

Related Commands

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

enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **enforcenextupdate** command in ca-crl configuration mode. To permit a lapsed or missing NextUpdate field, use the **no** form of this command.

enforcenextupdate

no enforcenextupdate

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is enforced (on).

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Ca-crl configuration	•	•	•	•	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

If set, this command requires CRLs to have a NextUpdate field that has not yet lapsed. If not used, the security appliance allows a missing or lapsed NextUpdate field in a CRL.

Examples

The following example enters ca-crl configuration mode, and requires CRLs to have a NextUpdate field that has not expired for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

Related Commands

Command	Description
cache-time	Specifies a cache refresh time in minutes.
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.

enrollment-retrieval

To specify the time in hours that an enrolled user can retrieve a PKCS12 enrollment file, use the **enrollment-retrieval** command in local ca server configuration mode. To reset the time to the default number of hours (24), use the **no** form of this command.

enrollment-retrieval *timeout*

no enrollment-retrieval

Syntax Description

timeout	Specifies the number of hours users have to retrieve an issued certificate from the local CA enrollment web page. Valid timeout values range from one to 720 hours.

Defaults

By default, the PKCS12 enrollment file is stored and retrievable for 24 hours.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A PKCS12 enrollment file contains an issued certificate and key pair. The file is stored on the local CA server and is available for retrieval from the enrollment web page for the time period specified with the **enrollment-retrieval** command.

When a user is marked as allowed to enroll, that user has **otp expiration** amount of time to enroll with that password. Once the user enrolls successfully, a PKCS12 file is generated, stored, and a copy is returned by way of the enrollment web page. The user can return for another copy of the file for any reason (such as when a download fails while trying enrollment) for the **enrollment-retrieval** command time period.

Note This time is independent from the OTP expiration period.

Examples

The following example specifies that a PKCS12 enrollment file is available for retrieval from the local CA server for 48 hours after the certificate is issued:

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

The following example resets the retrieval time back to the default of 24 hours:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
OTP expiration	Specifies the duration in hours that an issued one-time password for the CA enrollment page is valid.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the CA server.
smtp subject	Specifies the text appearing in the subject field of all e-mails generated by the local CA server.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

enrollment retry count

To specify a retry count, use the **enrollment retry count** command in crypto ca-trustpoint configuration mode. After requesting a certificate, the security appliance waits to receive a certificate from the CA. If the security appliance does not receive a certificate within the configured retry period, it sends another certificate request. The security appliance repeats the request until either it receives a response or reaches the end of the configured retry period. To restore the default setting of the retry count, use the **no** form of the command.

enrollment retry count *number*

no enrollment retry count

Syntax Description

number	The maximum number of attempts to send an enrollment request. The valid range is 0, 1-100 retries.

Defaults

The default setting for *number* is 0 (unlimited).

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	This command was introduced.

Usage Guidelines

This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and configures an enrollment retry count of 20 retries within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.

Command	Description
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.

enrollment retry period

To specify a retry period, use the **enrollment retry period** command in crypto ca trustpoint configuration mode. After requesting a certificate, the security appliance waits to receive a certificate from the CA. If the security appliance does not receive a certificate within the specified retry period, it sends another certificate request. To restore the default setting of the retry period, use the **no** form of the command.

enrollment retry period *minutes*

no enrollment retry period

Syntax Description

minutes	The number of minutes between attempts to send an enrollment request. The valid range is 1- 60 minutes.

Defaults

The default setting is 1 minute.

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	This command was introduced.

Usage Guidelines

This command is optional and applies only when automatic enrollment is configured.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and configures an enrollment retry period of 10 minutes within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns all enrollment parameters to their system default values.
enrollment retry count	Defines the number of retries to requesting an enrollment.

enrollment terminal

To specify cut and paste enrollment with this trustpoint (also known as manual enrollment), use the **enrollment terminal** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Defaults

The default setting is off.

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	This command was introduced.

Examples

The following example enters crypto ca-trustpoint configuration mode for trustpoint central, and specifies the cut and paste method of CA enrollment for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.
enrollment url	Specifies automatic enrollment (SCEP) with this trustpoint and configures the URL.

enrollment url

To specify automatic enrollment (SCEP) to enroll with this trustpoint and to configure the enrollment URL, use the **enrollment url** command in crypto ca-trustpoint configuration mode. To restore the default setting of the command, use the **no** form of the command.

enrollment url *url*

no enrollment url

Syntax Description

url	Specifies the name of the URL for automatic enrollment. The maximum length is 1K characters (effectively unbounded).

Defaults

The default setting is off.

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	This command was introduced.

Examples

The following example enters crypto ca-trustpoint configuration mode for trustpoint central, and specifies SCEP enrollment at the URL https://enrollsite for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before resending an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

enrollment-retrieval

To specify the time in hours that an enrolled user can retrieve a PKCS12 enrollment file, use the **enrollment-retrieval** command in local ca server configuration mode. To reset the time to the default number of hours (24), use the **no** form of this command.

enrollment-retrieval *timeout*

no enrollment-retrieval

Syntax Description

timeout	Specifies the number of hours users have to retrieve an issued certificate from the local CA enrollment web page. Valid timeout values range from one to 720 hours.

Defaults

By default, the PKCS12 enrollment file is stored and retrievable for 24 hours.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A PKCS12 enrollment file contains an issued certificate and key pair. The file is stored on the local CA server and is available for retrieval from the enrollment web page for the time period specified with the **enrollment-retrieval** command.

When a user is marked as allowed to enroll, that user has **otp expiration** amount of time to enroll with that password. Once the user enrolls successfully, a PKCS12 file is generated, stored, and a copy is returned by way of the enrollment web page. The user can return for another copy of the file for any reason (such as when a download fails while trying enrollment) for the **enrollment-retrieval** command time period.

Note This time is independent from the OTP expiration period.

Examples

The following example specifies that a PKCS12 enrollment file is available for retrieval from the local CA server for 48 hours after the certificate is issued:

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

The following example resets the retrieval time back to the default of 24 hours:

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

Related Commands

Command	Description
crypto ca server	Provides access to CA Server Configuration mode CLI command set, which allows you to configure and manage the local CA.
OTP expiration	Specifies the duration in hours that an issued one-time password for the CA enrollment page is valid.
smtp from-address	Specifies the e-mail address to use in the E-mail From: field for all e-mails generated by the CA server.
smtp subject	Specifies the text appearing in the subject field of all e-mails generated by the local CA server.
subject-name-default	Specifies a generic subject-name DN to be used along with the username in all user certificates issued by a CA server.

eou allow

To enable clientless authentication in a NAC Framework configuration, use the **eou allow** command in global configuration mode. To remove the command from the configuration, use the **no** form of this command.

eou allow {audit | clientless | none}

no eou allow {audit | clientless | none}

Syntax Description

audit	An audit server performs clientless authentication.
clientless	A Cisco ACS performs clientless authentication.
none	Disables clientless authentication.

Defaults

The default configuration contains the **eou allow clientless** 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
7.3(0)	Added the audit option.
7.2(1)	This command was introduced.

Usage Guidelines

The security appliance uses this command only if both of the following are true:

- The group policy is configured to use a nac-framework NAC policy type.
- A host on the session does not respond to EAPoUDP requests.

Examples

The following example enables the use of an ACS to perform clientless authentication:

```
hostname(config)# eou allow clientless
hostname(config)#
```

The following example shows how to configure the security appliance to use an audit server to perform clientless authentication:

```
hostname(config)# eou allow audit
hostname(config)#
```

The following example shows how to disable the use of an audit server:

```
hostname(config)# no eou allow clientless
hostname(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou clientless	Changes the username and password to be sent to the ACS for clientless authentication in a NAC Framework configuration.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou clientless

To change the username and password to be sent to the Access Control Server for clientless authentication in a NAC Framework configuration, use the **eou clientless** command in global configuration mode. To use the default value, use the **no** form of this command.

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

Syntax Description

password	Enter to change the password sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
password	Enter the password configured on the Access Control Server to support clientless hosts. Enter 4 – 32 ASCII characters.
username	Enter to change the username sent to the Access Control Server to obtain clientless authentication for a remote host that does not respond to EAPoUDP requests.
username	Enter the username configured on the Access Control Server to support clientless hosts. Enter 1 to 64 ASCII characters, excluding leading and trailing spaces, pound signs (#), question marks (?), quotation marks ("), asterisks (*), and angle brackets (< and >).

Defaults

The default value for both the username and password attributes is clientless.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.
- Clientless authentication is enabled on the security appliance.
- Network Admission Control is configured on the security appliance.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the username for clientless authentication to sherlock:

```
hostname(config)# eou clientless username sherlock
```

```
hostname(config)#
```

The following example changes the username for clientless authentication to the default value, clientless:

```
hostname(config)# no eou clientless username
hostname(config)#
```

The following example changes the password for clientless authentication to secret:

```
hostname(config)# eou clientless password secret
hostname(config)#
```

The following example changes the password for clientless authentication to the default value, clientless:

```
hostname(config)# no eou clientless password
hostname(config)#
```

Related Commands

Command	Description
eou allow	Enables clientless authentication in a NAC Framework configuration.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.

eou initialize

To clear the resources assigned to one or more NAC Framework sessions and initiate a new, unconditional posture validation for each of the sessions, use the **eou initialize** command in privileged EXEC mode.

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

Syntax Description

all	Revalidates all NAC Framework sessions on this security appliance
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Defaults

No default behavior or values.

Command Modes

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command if a change occurs in the posture of the remote peers or if the assigned access policies (that is, the downloaded ACLs) change, and you want to clear the resources assigned to the sessions. Entering this command purges the EAPoUDP associations and access policies used for posture validation. The NAC default ACL is effective during the revalidations, so the session initializations can disrupt user traffic. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example initializes all NAC Framework sessions:

```
hostname# eou initialize all
hostname
```

The following example initializes all NAC Framework sessions assigned to the tunnel group named tg1:

```
hostname# eou initialize group tg1
hostname
```

The following example initializes the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
hostname# eou initialize 209.165.200.225
hostname
```

Related Commands

Command	Description
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
debug nac	Enables logging of NAC Framework events.

eou max-retry

To change the number of times the security appliance resends an EAP over UDP message to the remote computer, use the **eou max-retry** command in global configuration mode. To use the default value, use the **no** form of this command.

eou max-retry *retries*

no eou max-retry

Syntax Description

retries	Limits the number of consecutive retries sent in response to retransmission timer expirations. Enter a value in the range 1 to 3.

Defaults

The default value is 3.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command is effective only if all of the following are true:

- An Access Control Server is configured on the network to support clientless authentication.
- Clientless authentication is enabled on the security appliance.
- Network Admission Control is configured on the security appliance.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example limits the number of EAP over UDP retransmissions to 1:

```
hostname(config)# eou max-retry 1
hostname(config)#
```

The following example changes the number of EAP over UDP retransmissions to its default value, 3:

```
hostname(config)# no eou max-retry
hostname(config)#
```

Related Commands

eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
debug nac	Enables logging of NAC Framework events.
show vpn-session.db	Displays information about VPN sessions, including NAC results.

eou port

To change the port number for EAP over UDP communication with the Cisco Trust Agent in a NAC Framework configuration, use the **eou port** command in global configuration mode. To use the default value, use the **no** form of this command.

eou port *port_number*

no eou port

Syntax Description

port_number	Port number on the client endpoint to be designated for EAP over UDP communications. This number is the port number configured on the Cisco Trust Agent. Enter a value in the range 1024 to 65535.

Defaults

The default value is 21862.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the port number for EAP over UDP communication to 62445:

```
hostname(config)# eou port 62445
hostname(config)#
```

The following example changes the port number for EAP over UDP communication to its default value:

```
hostname(config)# no eou port
hostname(config)#
```

Related Commands

debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou revalidate	Forces immediate posture revalidation of one or more NAC Framework sessions.
show vpn-session_summary.db	Displays the number IPSec, Cisco AnyConnect, and NAC sessions, including VLAN mapping session data.
show vpn-session.db	Displays information about VPN sessions, including VLAN mapping and NAC results.

eou revalidate

To force immediate posture revalidation of one or more NAC Framework sessions, use the **eou revalidate** command in privileged EXEC mode.

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

Syntax Description

all	Revalidates all NAC Framework sessions on this security appliance
group	Revalidates all NAC Framework sessions assigned to a tunnel group.
ip	Revalidates a single NAC Framework session.
ip-address	IP address of the remote peer end of the tunnel.
tunnel-group	Name of the tunnel group used to negotiate parameters to set up the tunnel.

Defaults

No default behavior or values.

Command Modes

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Use this command if the posture of the peer or the assigned access policy (that is, the downloaded ACL, if any) has changed. The command initiates a new, unconditional posture validation. The posture validation and assigned access policy that were in effect before you entered the command remain in effect until the new posture validation succeeds or fails. This command does not affect peers that are exempt from posture validation.

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example revalidates all NAC Framework sessions:

```
hostname# eou revalidate all
hostname
```

The following example revalidates all NAC Framework sessions assigned to the tunnel group named tg-1:

```
hostname# eou revalidate group tg-1
hostname
```

The following example revalidates the NAC Framework session for the endpoint with the IP address 209.165. 200.225:

```
hostname# eou revalidate ip 209.165.200.225
hostname
```

Related Commands

Command	Description
eou initialize	Clears the resources assigned to one or more NAC Framework sessions and initiates a new, unconditional posture validation for each of the sessions.
eou timeout	Changes the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration.
reval-period	Specifies the interval between each successful posture validation in a NAC Framework session.
sq-period	Specifies the interval between each successful posture validation in a NAC Framework session and the next query for changes in the host posture.
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.

eou timeout

To change the number of seconds to wait after sending an EAP over UDP message to the remote host in a NAC Framework configuration, use the **eou timeout** command in global configuration mode. To use the default value, use the **no** form of this command.

eou timeout {**hold-period | retransmit**} *seconds*

no eou timeout {**hold-period | retransmit**}

Syntax Description

hold-period	Maximum time to wait after sending EAPoUDP messages equal to the number of EAPoUDP retries. The **eou initialize** or **eou revalidate** command also clears this timer. If this timer expires, the security appliance initiates a new EAP over UDP association with the remote host.
retransmit	Maximum time to wait after sending an EAPoUDP message. A response from the remote host clears this timer. The **eou initialize** or **eou revalidate** command also clears this timer. If the timer expires, the security appliance retransmits the EAPoUDP message to the remote host.
seconds	Number of seconds for the security appliance to wait. Enter a value in the range 60 to 86400 for the hold-period attribute, or the range 1 to 60 for the retransmit attribute.

Defaults

The default value of the hold-period attribute is 180.

The default value of the retransmit attribute is 3.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command applies only to the Framework implementation of Cisco NAC.

Examples

The following example changes the wait period before initiating a new EAP over UDP association to 120 seconds:

```
hostname(config)# eou timeout hold-period 120
hostname(config)#
```

The following example changes the wait period before initiating a new EAP over UDP association to its default value:

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

The following example changes the retransmission timer to 6 seconds:

```
hostname(config)# eou timeout retransmit 6
hostname(config)#
```

The following example changes the retransmission timer to its default value:

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

Related Commands

Command	Description
debug eou	Enables logging of EAP over UDP events to debug NAC Framework messaging.
eou max-retry	Changes the number of times the security appliance resends an EAP over UDP message to the remote computer.

erase

To erase and reformat the file system, use the **erase** command in privileged EXEC mode. This command overwrites all files and erases the file system, including hidden system files, and then reinstalls the file system.

erase [**disk0: | disk1: | flash:**]

Syntax Description

disk0*:*	(Optional) Specifies the internal Flash memory, followed by a colon.
disk1:	(Optional) Specifies the external, compact Flash memory card, followed by a colon.
flash:	(Optional) Specifies the internal Flash memory, followed by a colon. **Caution** Erasing the Flash memory also removes the licensing information, which is stored in Flash memory. Save the licensing information prior to erasing the Flash memory. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Defaults

This command has no default settings.

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	This command was introduced.

Usage Guidelines

The **erase** command erases all data on the Flash memory using the OxFF pattern and then rewrites an empty file system allocation table to the device.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **erase** command.

Note On Cisco PIX security appliances, the **erase** and **format** commands do the same thing, destroy user data with the 0xFF pattern.

Note On Cisco ASA 5500 series security appliances, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information.

Examples

The following example erases and reformats the file system:

```
hostname# erase flash:
```

Related Commands

Command	Description
delete	Removes all visible files, excluding hidden system files.
format	Erases all files (including hidden system files) and formats the file system.

esp

To specify parameters for esp and AH tunnels for IPSec Pass Thru inspection, use the **esp** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

Syntax Description

esp	Specifies parameters for esp tunnel.
ah	Specifies parameters for AH tunnel.
per-client-max *num*	Specifies maximum tunnels from one client.
timeout *time*	Specifies idle timeout for the esp tunnel.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Examples

The following example shows how to permit UDP 500 traffic:

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-pmap-c)# match access-list test-udp-acl

hostname(config)# policy-map type inspect ipsec-pass-thru ipsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

Related Commands

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

established

To permit return connections on ports that are based on an established connection, use the **established** command in global configuration mode. To disable the **established** feature, use the **no** form of this command.

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

Syntax Description

est_protocol	Specifies the IP protocol (UDP or TCP) to use for the established connection lookup.
dest_port	Specifies the destination port to use for the established connection lookup.
permitfrom	(Optional) Allows the return protocol connection(s) originating from the specified port.
permitto	(Optional) Allows the return protocol connections destined to the specified port.
port [*-port*]	(Optional) Specifies the (UDP or TCP) destination port(s) of the return connection.
protocol	(Optional) IP protocol (UDP or TCP) used by the return connection.
source_port	(Optional) Specifies the source port to use for the established connection lookup.

Defaults

The defaults are as follows:

- *dest_port*—0 (wildcard)
- *source_port*—0 (wildcard)

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)	The keywords **to** and **from** were removed from the CLI. Use the keywords **permitto** and **permitfrom** instead.

Usage Guidelines

The **established** command lets you permit return access for outbound connections through the security appliance. This command works with an original connection that is outbound from a network and protected by the security appliance and a return connection that is inbound between the same two devices on an external host. The **established** command lets you specify the destination port that is used for

connection lookups. This addition allows more control over the command and provides support for protocols where the destination port is known, but the source port is unknown. The **permitto** and **permitfrom** keywords define the return inbound connection.

Caution We recommend that you always specify the **established** command with the **permitto** and **permitfrom** keywords. Using the **established** command without these keywords is a security risk because when connections are made to external systems, those system can make unrestricted connections to the internal host involved in the connection. This situation can be exploited for an attack of your internal systems.

Examples

The following set of examples shows potential security violations could occur if you do not use the **established** command correctly.

This example shows that if an internal system makes a TCP connection to an external host on port 4000, then the external host could come back in on any port using any protocol:

```
hostname(config)# established tcp 4000 0
```

You can specify the source and destination ports as **0** if the protocol does not specify which ports are used. Use wildcard ports (0) only when necessary.

```
hostname(config)# established tcp 0 0
```

Note To allow the **established** command to work properly, the client must listen on the port that is specified with the **permitto** keyword.

You can use the **established** command with the **nat 0** command (where there are no **global** commands).

Note You cannot use the **established** command with PAT.

The security appliance supports XDMCP with assistance from the **established** command.

Caution Using XWindows system applications through the security appliance may cause security risks.

XDMCP is on by default, but it does not complete the session unless you enter the **established** command as follows:

```
hostname(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

Entering the **established** command enables the internal XDMCP-equipped (UNIX or ReflectionX) hosts to access external XDMCP-equipped XWindows servers. UDP/177-based XDMCP negotiates a TCP-based XWindows session, and subsequent TCP back connections are permitted. Because the source port(s) of the return traffic is unknown, specify the *source_port* field as 0 (wildcard). The *dest_port* should be 6000 + *n*, where *n* represents the local display number. Use this UNIX command to change this value:

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

The **established** command is needed because many TCP connections are generated (based on user interaction) and the source port for these connections is unknown. Only the destination port is static. The security appliance performs XDMCP fixups transparently. No configuration is required, but you must enter the **established** command to accommodate the TCP session.

The following example shows a connection between two hosts using protocol A destined for port B from source port C. To permit return connections through the security appliance and protocol D (protocol D can be different from protocol A), the source port(s) must correspond to port F and the destination port(s) must correspond to port E.

```
hostname(config)# established A B C permitto D E permitfrom D F
```

The following example shows how a connection is started by an internal host to an external host using TCP destination port 6060 and any source port. The security appliance permits return traffic between the hosts through TCP destination port 6061 and any TCP source port.

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

The following example shows how a connection is started by an internal host to an external host using UDP destination port 6060 and any source port. The security appliance permits return traffic between the hosts through TCP destination port 6061 and TCP source port 1024-65535.

```
hostname(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

The following example shows how a local host starts a TCP connection on port 9999 to a foreign host. The example allows packets from the foreign host on port 4242 back to local host on port 5454.

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

Related Commands

Command	Description
clear configure established	Removes all established commands.
show running-config established	Displays the allowed inbound connections that are based on established connections.

exceed-mss

To allow or drop packets whose data length exceeds the TCP maximum segment size set by the peer during a three-way handshake, use the **exceed-mss** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

Syntax Description

allow	Allows packets that exceed the MSS. This setting is the default.
drop	Drops packets that exceed the MSS.

Defaults

Packets are allowed by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
7.2(4)/8.0(4)	The default was changed from **drop** to **allow**.

Usage Guidelines

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **exceed-mss** command in tcp-map configuration mode to drop TCP packets whose data length exceed the TCP maximum segment size set by the peer during a three-way handshake.

Examples

The following example drops flows on port 21 if they are in excess of MSS:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss drop
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

Related Commands

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

exempt-list

To add an entry to the list of remote computer types that are exempt from posture validation, use the **exempt-list** command in nac-policy-nac-framework configuration mode. To remove an entry from the exemption list, use the **no** form of this command and name the operating system, and ACL, in the entry to be removed.

exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

Syntax Description

acl-name	Name of the ACL present in the security appliance configuration. When specified, it must follow the **filter** keyword.
disable	Performs one of two functions, as follows: • If you enter it after the "os-name," the security appliance ignores the exemption, and applies NAC posture validation to the remote hosts that are running that operating system. • If you enter it after the *acl-name*, security appliance exempts the operating system, but does not assign the ACL to the associated traffic.
filter	Applies an ACL to filter the traffic if the computer's operating system matches the *os name*. The **filter**/*acl-name* pair is optional.
os	Exempts an operating system from posture validation.
os name	Operating system name. Quotation marks are required only if the name includes a space (for example, `"Windows XP"`).

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**
nac-policy-nac-framework configuration	•	—	•	—	—

Command History

Release	Modification
7.3(0)	Command name changed from **vpn-nac-exempt** to **exempt-list**. Command moved from group-policy configuration mode to nac-policy-nac-framework configuration mode.
7.2(1)	This command was introduced.

Usage Guidelines

When the command specifies an operating system, it does not overwrite the previously added entry to the exception list; enter the command once for each operating system and ACL you want to exempt.

The **no exempt-list** command removes all exemptions from the NAC Framework policy. Specifying an entry when issuing the **no** form of the command removes the entry from the exemption list.

To remove all entries from the exemption list associated with this NAC policy, use the **no** form of this command without specifying additional keywords.

Examples

The following example adds all hosts running Windows XP to the list of computers that are exempt from posture validation:

```
hostname(config-group-policy)# exempt-list os "Windows XP"
hostname(config-group-policy)
```

The following example exempts all hosts running Windows XP and applies the ACL acl-1 to traffic from those hosts:

```
hostname(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

The following example removes the same entry from the exemption list:

```
hostname(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

The following example removes all entries from the exemption list:

```
hostname(config-nac-policy-nac-framework)# no exempt-list
hostname(config-nac-policy-nac-framework)
```

Related Commands

Command	Description
nac-policy	Creates and accesses a Cisco NAC policy, and specifies its type.
nac-settings	Assigns a NAC policy to a group policy.
show vpn-session_summary.db	Displays the number IPSec, Cisco AnyConnect, and NAC sessions.
show vpn-session.db	Displays information about VPN sessions, including NAC results.
debug nac	Enables logging of NAC Framework events.

exit

To exit the current configuration mode, or to logout from privileged or user EXEC modes, use the **exit** command.

exit

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
User EXEC	•	•	•	•	•

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

You can also use the key sequence **Ctrl Z** to exit global configuration (and higher) modes. This key sequence does not work with privileged or user EXEC modes.

When you enter the **exit** command in privileged or user EXEC modes, you log out from the security appliance. Use the **disable** command to return to user EXEC mode from privileged EXEC mode.

Examples

The following example shows how to use the **exit** command to exit global configuration mode, and then logout from the session:

```
hostname(config)# exit
hostname# exit

Logoff
```

The following example shows how to use the **exit** command to exit global configuration mode, and then use the **disable** command to exit privileged EXEC mode:

```
hostname(config)# exit
hostname# disable
hostname>
```

Related Commands

Command	Description
quit	Exits a configuration mode or logs out from privileged or user EXEC modes.

expiry-time

To configure an expiration time for caching objects without revalidating them, use the **expiry-time** command in cache configuration mode. To remove the expiration time from the configuration and reset it to the default value, use the **no** form of this command.

expiry-time *time*

no expiry-time

Syntax Description

time	The amount of time in minutes that the security appliance caches objects without revalidating them.

Defaults

One minute.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The expiration time is the amount of time in minutes that the security appliance caches an object without revalidating it. Revalidation consists of rechecking the content.

Examples

The following example shows how to set an expiration time with a value of 13 minutes:

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#expiry-time 13
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
disable	Disables caching.

Command	Description
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum sizze of an object to cache.

export

To specify the certificate to be exported to the client, use the **export** command in CTL provider configuration mode. To remove the configuration, use the **no** form of this command.

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

Syntax Description

certificate *trustpoint_name*	Specifies the certificate to be exported to the client.

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 provider configuration	•	•	•	•	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Use the **export** command in CTL provider configuration mode to specify the certificate to be exported to the client. The trustpoint name is defined by the **crypto ca trustpoint** command. The certificate will be added to the Certificate Trust List file composed by the CTL client.

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
ctl	Parses the CTL file from the CTL client and install trustpoints.
ctl-provider	Configures a CTL provider instance in CTL provider mode.
client	Specifies clients allowed to connect to the CTL provider and also username and password for client authentication.

Commands	Description
service	Specifies the port to which the CTL provider listens.
tls-proxy	Defines a TLS proxy instance and sets the maximum sessions.

export webvpn customization

To export a customization object that customizes screens visible to Clientless SSL VPN users, use the **export webvpn customization** command from privileged EXEC mode.

export webvpn customization *name url*

Syntax Description

name	The name that identifies the customization object. Maximum 64 characters.
url	Remote path and filename to export the XML customization object, in the form *URL/filename* (maximum 255 characters).

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

A customization object is an XML file that resides in cache memory, and customizes the screens visible to Clientless SSL VPN users, including logon and logout screens, the portal page, and available languages. When you export a customization object, an XML file containing XML tags is created at the URL you specify.

The XML file created by the customization object named *Template* contains empty XML tags, and provides the basis for creating new customization objects. This object cannot be changed or deleted from cache memory, but can be exported, edited, and imported back into the security appliance as a new customization object.

The content of Template is the same as the initial DfltCustomization object state.

You can export a customization object using the **export webvpn customization** command, make changes to the XML tags, and import the file as a new object using the **import webvpn customization** command.

Examples

The following example exports the default customization object (DfltCustomization) and creates the resulting XML file named dflt_custom:

```
hostname# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
```

```
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
hostname#
```

Related Commands

Command	Description
import webvpn customization	Imports an XML file to cache memory as a customization object .
revert webvpn customization	Removes a customization object from cache memory.
show import webvpn customization	Displays information about customization objects resident in cache memory.

export webvpn translation-table

To export a translation table used to translate terms displayed to remote users establishing SSL VPN connections, use the **export webvpn translation-table** command from privileged EXEC mode.

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

Syntax Description

language	Specifies the name of a previously-imported translation table. Enter the value in the manner expressed by your browser language options.
translation_domain	The functional area and associated messages. The usage guidelines section lists available translation domains.
url	Specifies the URL of the object.

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance provides language translation for the portal and screens displayed to users that initiate browser-based, clientless SSL VPN connections, as well as the user interface displayed to AnyConnect VPN Client users.

Each functional area and its messages that is visible to remote users has its own translation domain and is specified by the *translation_domain* argument. The following table shows the translation domains and the functional areas translated.

Table 12-1 Translation Domains and Functional Areas Affected

Translation Domain	Functional Areas Translated
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.
CSD	Messages for the Cisco Secure Desktop (CSD).
customization	Messages on the logon and logout pages, portal page, and all the messages customizable by the user.

Translation Domain	Functional Areas Translated
banners	Banners displayed to remote users and messages when VPN access is denied.
PortForwarder	Messages displayed to Port Forwarding users.
url-list	Text that user specifies for URL bookmarks on the portal page.
webvpn	All the layer 7, AAA and portal messages that are not customizable.
plugin-ica	Messages for the Citrix plug-in.
plugin-rdp	Messages for the Remote Desktop Protocol plug-in.
plugin-telnet,ssh	Messages for the Telnet and SSH plug-in.
plugin-vnc	Messages for the VNC plug-in.
AnyConnect	Messages displayed on the user interface of the Cisco AnyConnect VPN Client.

A translation template is an XML file in the same format as the translation table, but has all the translations empty. The software image package for the security appliance includes a template for each domain that is part of the standard functionality. Templates for plug-ins are included with the plug-ins and define their own translation domains. Because you can customize the logon and logout pages, portal page, and URL bookmarks for clientless users, the security appliance generates the **customization** and **url-list** translation domain templates dynamically and the template automatically reflects your changes to these functional areas.

Exporting a previously-imported translation table creates an XML file of the table at the URL location. You can view a list of available templates and previously-imported tables using the **show import webvpn translation-table** command.

Download a template or translation table using the **export webvpn translation-table** command, make changes to the messages, and import the translation table using the **import webvpn translation-table** command.

Examples

The following example exports a template for the translation domain *customization*, which is used to translate the logon and logout pages, portal page, and all the messages customizable and visible to remote users establishing clientless SSL VPN connections. The security appliance creates the XML file with the name *Sales*:

```
hostname# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

The next example exports a previously-imported translation table for the Chinese language named *zh*, an abbreviation compatible with the abbreviation specified for Chinese in the Internet Options of the Microsoft Internet Explorer browser. The security appliance creates the XML file with the name *Chinese*:

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Related Commands

Command	Description
import webvpn translation-table	Imports a translation table.
revert	Removes translation tables from cache memory.
show import webvpn translation-table	Displays information about imported translation tables.

export webvpn url-list

To export a URL list to a remote location, use the **export webvpn url-list** command from privileged EXEC mode.

export webvpn url-list *name url*

Syntax Description

name	The name that identifies the URL list. Maximum 64 characters.
URL	Remote path to the source of the URL list. Maximum 255 characters.

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

No URL lists are present in WebVPN by default.

An object, Template, is available for downloading with the **export webvpn url-list** command. Template cannot be changed or deleted. The contents of Template can be edited and saved as a custom URL list, and imported with the **import webvpn url-list** command to add a custom URL list.

Exporting a previously-imported URL list creates an XML file of the list at the URL location. You can view a list of available templates and previously-imported tables using the **show import webvpn url-list** command.

Examples

The following example exports a URL list, *servers*:

```
hostname# export webvpn url-list servers2 tftp://209.165.200.225
hostname#
```

Related Commands

Command	Description
import webvpn url-list	Imports a URL list.

revert webvpn url-list	Removes URL lists from cache memory.
show import webvpn url-list	Displays information about imported URL lists.

export webvpn webcontent

To export previously-imported content in flash memory that is visible to remote Clientless SSL VPN users, use the **export webvpn webcontent** command from privileged EXEC mode.

export webvpn webcontent <*source url*> <*destination url*>

Syntax Description

<*source url*>	The URL in the security appliance flash memory where the content resides. See Maximum 64 characters.
<*destination url*>	The URL to export to. Maximum 255 characters.

Defaults

There is no default behavior for this command.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

Content exported with the **webcontent** option is content visible to remote Clientless users. This includes previously-imported help content visible on the Clientless portal and logos used by customization objects.

You can see a list of content available for export by entering a question mark (**?**) after the **export webvpn webcontent** command. For example:

```
hostname# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

Examples

The following example exports the file *logo.gif*, using tftp, to 209.165.200.225, as the filename *logo_copy.gif*:

```
hostname# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

Related Commands

Command	Description
import webvpn webcontent	Imports content visible to Clientless SSL VPN users.
revert webvpn webcontent	Removes content from flash memory.
show import webvpn webcontent	Displays information about imported content.

failover

To enable failover, use the **failover** command in global configuration mode. To disable failover, use the **no** form of this command.

failover

no failover

Syntax Description

This command has no arguments or keywords.

Defaults

Failover 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
7.0(1)	This command was limited to enable or disable failover in the configuration (see the **failover active** command).

Usage Guidelines

Use the **no** form of this command to disable failover.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

The ASA 5505 device allows only Stateless Failover, and only while not acting as an Easy VPN hardware client.

Examples

The following example disables failover:

```
hostname(config)# no failover
hostname(config)#
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover active	Switches the standby unit to active.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover active

To switch a standby security appliance or failover group to the active state, use the **failover active** command in privileged EXEC mode. To switch an active security appliance or failover group to standby, use the **no** form of this command.

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

Syntax Description

group *group_id*	(Optional) Specifies the failover group to make active.

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 modified to include failover groups.

Usage Guidelines

Use the **failover active** command to initiate a failover switch from the standby unit, or use the **no failover active** command from the active unit to initiate a failover switch. You can use this feature to return a failed unit to service, or to force an active unit offline for maintenance. If you are not using stateful failover, all active connections are dropped and must be reestablished by the clients after the failover occurs.

Switching for a failover group is available only for Active/Active failover. If you enter the **failover active** command on an Active/Active failover unit without specifying a failover group, all groups on the unit become active.

Examples

The following example switches the standby group 1 to active:

```
hostname# failover active group 1
```

Related Commands

Command	Description
failover reset	Moves a security appliance from a failed state to standby.

failover exec

To execute a command on a specific unit in a failover pair, use the **failover exec** command in privileged EXEC or global configuration mode.

failover exec {**active** | **standby** | **mate**} *cmd_string*

Syntax Description

active	Specifies that the command is executed on the active unit or failover group in the failover pair. Configuration commands entered on the active unit or failover group are replicated to the standby unit or failover group.
cmd_string	The command to be executed. Show, configuration, and exec commands are supported.
mate	Specifies that the command is executed on the failover peer.
standby	Specifies that the command is executed on the standby unit or failover group in the failover pair. Configuration commands executed on the standby unit or failover group are not replicated to the active unit or failover group.

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**
Privileged EXEC	•	•	•	•	•

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

You can use the **failover exec** command to send commands to a specific unit in a failover pair.

Because configuration commands are replicated from the active unit or context to the standby unit or context, you can use the **failover exec** command to enter configuration commands on the correct unit, no matter which unit you are logged-in to. For example, if you are logged-in to the standby unit, you can use the **failover exec active** command to send configuration changes to the active unit. Those changes are then replicated to the standby unit. Do not use the **failover exec** command to send configuration commands to the standby unit or context; those configuration changes are not replicated to the active unit and the two configurations will no longer be synchronized.

Output from configuration, exec, and **show** commands is displayed in the current terminal session, so you can use the **failover exec** command to issue **show** commands on a peer unit and view the results in the current terminal.

You must have sufficient privileges to execute a command on the local unit to execute the command on the peer unit.

Command Modes

The **failover exec** command maintains a command mode state that is separate from the command mode of your terminal session. By default, the **failover exec** command mode is global configuration mode for the specified device. You can change that command mode by sending the appropriate command (such as the **interface** command) using the **failover exec** command.

Changing **failover exec** command modes for the specified device does not change the command mode for the session you are using to access the device. For example, if you are logged-in to the active unit of a failover pair, and you issue the following command from global configuration mode, you will remain in global configuration mode but any commands sent using the **failover exec** command will be executed in interface configuration mode:

```
hostname(config)# failover exec interface GigabitEthernet0/1
hostname(config)#
```

Changing commands modes for your current session to the device does not affect the command mode used by the **failover exec** command. For example, if you are in interface configuration mode on the active unit, and you have not changed the **failover exec** command mode, the following command would be executed in global configuration mode:

```
hostname(config-if)# failover exec active router ospf 100
hostname(config-if)#
```

Use the **show failover exec** command to display the command mode on the specified device in which commands sent with the **failover exec** command are executed.

Security Considerations

The **failover exec** command uses the failover link to send commands to and receive the output of the command execution from the peer unit. You should use the **failover key** command to encrypt the failover link to prevent eavesdropping or man-in-the-middle attacks.

Limitations

- If you upgrade one unit using the zero-downtime upgrade procedure and not the other, both units must be running software that supports the **failover exec** command for the command to work.
- Command completion and context help is not available for the commands in the *cmd_string* argument.
- In multiple context mode, you can only send commands to the peer context on the peer unit. To send commands to a different context, you must first change to that context on the unit you are logged-in to.
- You cannot use the following commands with the **failover exec** command:
  - **changeto**
  - **debug** (**undebug**)
- If the standby unit is in the failed state, it can still receive commands from the **failover exe**c command if the failure is due to a service card failure; otherwise, the remote command execution will fail.
- You cannot use the **failover exec** command to switch from privileged EXEC mode to global configuration mode on the failover peer. For example, if the current unit is in privileged EXEC mode, and you enter **failover exec mate configure terminal**, the **show failover exec mate** output

will show that the failover exec session is in global configuration mode. However, entering configuration commands for the peer unit using **failover exec** will fail until you enter global configuration mode on the current unit.

- You cannot enter recursive failover exec commands, such as **failover exec mate failover exec mate** *command*.
- Commands that require user input or confirmation must use the **/nonconfirm** option.

Examples

The following example shows how to use the **failover exec** command to display failover information on the active unit. The unit on which the command is executed is the active unit, so the command is executed locally.

```
hostname(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
hostname(config)#
```

The following example uses the **failover exec** command to display the failover status of the peer unit. The command is executed on the the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
hostname(config)# failover exec mate show failover
```

```
Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

The following example uses the **failover exec** command to display the failover configuration of the failover peer. The command is executed on the primary unit, which is the active unit, so the information displayed is from the secondary, standby unit.

```
hostname(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

The following example uses the **failover exec** command to create a context on the active unit from the standby unit. The command is replicated from the active unit back to the standby unit. Note the two "Creating context…" messages. One is from the **failover exec** command output from the peer unit when the context is created, and the other is from the local unit when the replicated command creates the context locally.

```
hostname(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

hostname(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

hostname(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

The following example shows the warning that is returned when you use the **failover exec** command to send configuration commands to a failover peer in the standby state:

```
hostname# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

       **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
hostname(config)#
```

The following example uses the **failover exec** command to send the **show interface** command to the standby unit:

```
hostname(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
      284 packets output, 26976 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  23 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  24 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
```

```
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
      MAC address 000b.fcf8.c291, MTU 1500
      IP address 192.168.0.11, subnet mask 255.255.255.0
      214 packets input, 26902 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      215 packets output, 27028 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
      214 packets input, 23050 bytes
      215 packets output, 23140 bytes
      0 packets dropped
      1 minute input rate 0 pkts/sec,  21 bytes/sec
      1 minute output rate 0 pkts/sec,  21 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  21 bytes/sec
      5 minute output rate 0 pkts/sec,  21 bytes/sec
      5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
      Description: LAN/STATE Failover Interface
      MAC address 000b.fcf8.c293, MTU 1500
      IP address 10.0.5.2, subnet mask 255.255.255.0
      1991 packets input, 408734 bytes, 0 no buffer
      Received 1 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      1835 packets output, 254114 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
      1913 packets input, 345310 bytes
      1755 packets output, 212452 bytes
      0 packets dropped
      1 minute input rate 1 pkts/sec,  319 bytes/sec
      1 minute output rate 1 pkts/sec,  194 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 1 pkts/sec,  318 bytes/sec
      5 minute output rate 1 pkts/sec,  192 bytes/sec
      5 minute drop rate, 0 pkts/sec
.
.
.
```

The following example shows the error message returned when issuing an illegal command to the peer unit:

```
hostname# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

The following example shows the error message that is returned when you use the **failover exec** command when failover is disabled:

```
hostname(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

Related Commands

Command	Description
debug fover	Displays failover-related debug messages.
debug xml	Displays debug messages for the XML parser used by the **failover exec** command.
show failover exec	Displays the **failover exec** command mode.

failover group

To configure an Active/Active failover group, use the **failover group** command in global configuration mode. To remove a failover group, use the **no** form of this command.

failover group *num*

no failover group *num*

Syntax Description

num	Failover group number. Valid values are 1 or 2.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can define a maximum of 2 failover groups. The **failover group** command can only be added to the system context of devices configured for multiple context mode. You can create and remove failover groups only when failover is disabled.

Entering this command puts you in the failover group command mode. The **primary**, **secondary**, **preempt**, **replication http**, **interface-policy**, **mac address**, and **polltime interface** commands are available in the failover group configuration mode. Use the **exit** command to return to global configuration mode.

Note The **failover polltime interface**, **failover interface-policy**, **failover replication http**, and **failover mac address** commands have no effect in Active/Active failover configurations. They are overridden by the following failover group configuration mode commands: **polltime interface**, **interface-policy**, **replication http**, and **mac address**.

When removing failover groups, you must remove failover group 1 last. Failover group 1 always contains the admin context. Any context not assigned to a failover group defaults to failover group 1. You cannot remove a failover group that has contexts explicitly assigned to it.

Note If you have more than one Active/Active failover pair on the same network, it is possible to have the same default virtual MAC addresses assigned to the interfaces on one pair as are assigned to the interfaces of the other pairs because of the way the default virtual MAC addresses are determined. To avoid having duplicate MAC addresses on your network, make sure you assign each physical interface a virtual active and standby MAC address using the **mac address** command.

Examples

The following partial example shows a possible configuration for two failover groups:

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

Related Commands

Command	Description
asr-group	Specifies an asymmetrical routing interface group ID.
interface-policy	Specifies the failover policy when monitoring detects interface failures.
join-failover-group	Assigns a context to a failover group.
mac address	Defines virtual mac addresses for the contexts within a failover group.
polltime interface	Specifies the amount of time between hello messages sent to monitored interfaces.
preempt	Specifies that a unit with a higher priority becomes the active unit after a reboot.
primary	Gives the primary unit higher priority for a failover group.
replication http	Specifies HTTP session replication for the selected failover group.
secondary	Gives the secondary unit higher priority for a failover group.

failover interface ip

To specify the IP address and mask for the failover interface and the Stateful Failover interface, use the **failover interface ip** command in global configuration mode. To remove the IP address, use the **no** form of this command.

failover interface ip *if_name ip_address mask* **standby** *ip_address*

no failover interface ip *if_name ip_address mask* **standby** *ip_address*

Syntax Description

if_name	Interface name for the failover or stateful failover interface.
ip_address mask	Specifies the IP address and mask for the failover or stateful failover interface on the primary module.
standby *ip_address*	Specifies the IP address used by the secondary module to communicate with the primary module.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Failover and stateful failover interfaces are functions of Layer 3, even when the security appliance is operating in transparent firewall mode, and are global to the system.

In multiple context mode, you configure failover in the system context (except for the **monitor-interface** command).

This command must be part of the configuration when bootstrapping a security appliance for LAN failover.

Examples

The following example shows how to specify the IP address and mask for the failover interface:

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

Related Commands

Command	Description
clear configure failover	Clears **failover** commands from the running configuration and restores failover default values.
failover lan interface	Specifies the interface used for failover communication.
failover link	Specifies the interface used for Stateful Failover.
monitor-interface	Monitors the health of the specified interface.
show running-config failover	Displays the **failover** commands in the running configuration.

failover interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **failover interface-policy** command in global configuration mode. To restore the default, use the **no** form of this command.

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces when used as a number.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Defaults

The defaults are as follows:

- *num* is 1.
- Monitoring of physical interfaces is enabled by default; monitoring of logical interfaces is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other security appliance is functioning properly, the security appliance marks itself as failed and a failover might occur (if the active security appliance is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the interface policy for each failover group with the **interface-policy** command in failover group configuration mode.

Examples

The following examples show two ways to specify the failover policy:

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit and interface poll times.
failover reset	Restores a failed unit to an unfailed state.
monitor-interface	Specifies the interfaces being monitored for failover.
show failover	Displays information about the failover state of the unit.

failover key

To specify the key for encrypted and authenticated communication between units in a failover pair, use the **failover key** command in global configuration mode. To remove the key, use the **no** form of this command.

failover key {*secret* | **hex** *key*}

no failover key

Syntax Description

hex *key*	Specifies a hexadecimal value for the encryption key. The key must be 32 hexadecimal characters (0-9, a-f).
secret	Specifies an alphanumeric shared secret. The secret can be from 1 to 63 characters. Valid character are any combination of numbers, letters, or punctuation. The shared secret is used to generate the encryption key.

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 modified from **failover lan key** to **failover key**.
7.0(4)	This command was modified to include the **hex** *key* keyword and argument.

Usage Guidelines

To encrypt and authenticate failover communications between the units, you must configure both units with a shared secret or hexadecimal key. If you do not specify a failover key, failover communication is transmitted in the clear.

Note On the PIX security appliance platform, if you are using the dedicated serial failover cable to connect the units, then communication over the failover link is not encrypted even if a failover key is configured. The failover key only encrypts LAN-based failover communication.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels.

Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example shows how to specify a shared secret for securing failover communication between units in a failover pair:

```
hostname(config)# failover key abcdefg
```

The following example shows how to specify a hexadecimal key for securing failover communication between two units in a failover pair:

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

Related Commands

Command	Description
show running-config failover	Displays the failover commands in the running configuration.

failover lan enable

To enable lan-based failover on the PIX security appliance, use the **failover lan enable** command in global configuration mode. To disable LAN-based failover, use the **no** form of this command.

failover lan enable

no failover lan enable

Syntax Description

This command has no arguments or keywords.

Defaults

Not enabled.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When LAN-based failover is disabled using the **no** form of this command, cable-based failover is used if the failover cable is installed. This command is available on the PIX security appliance only.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any usernames, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example enables LAN-based failover:

```
hostname(config)# failover lan enable
```

Related Commands

Command	Description
failover lan interface	Specifies the interface used for failover communication.
failover lan unit	Specifies the LAN-based failover primary or secondary unit.
show failover	Displays information about the failover status of the unit.
show running-config failover	Displays the **failover** commands in the running configuration.

failover lan interface

To specify the interface used for failover communication, use the **failover lan interface** command in global configuration mode. To remove the failover interface, use the **no** form of this command.

failover lan interface *if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[.*sub_if*] | *vlan_if*]}]

Syntax Description

if_name	Specifies the name of the security appliance interface dedicated to failover.
phy_if	Specifies the physical interface.
sub_if	(Optional) Specifies a subinterface number.
vlan_if	Used on the ASA 5505 adaptive security appliance to specify a VLAN interface as the failover link.

Defaults

Not configured.

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 modified to include the *phy_if* argument.
7.2(1)	This command was modified to include the *vlan_if* argument.

Usage Guidelines

LAN failover requires a dedicated interface for passing failover traffic. However you can also use the LAN failover interface for the Stateful Failover link.

Note If you use the same interface for both LAN failover and Stateful Failover, the interface needs enough capacity to handle both the LAN-based failover and Stateful Failover traffic.

You can use any unused Ethernet interface on the device as the failover interface. You cannot specify an interface that is currently configured with a name. The failover interface is not configured as a normal networking interface; it exists only for failover communications. This interface should only be used for the failover link (and optionally for the state link). You can connect the LAN-based failover link by using a dedicated switch with no hosts or routers on the link or by using a crossover Ethernet cable to link the units directly.

Note When using VLANs, use a dedicated VLAN for the failover link. Sharing the failover link VLAN with any other VLANs can cause intermittent traffic problems and ping and ARP failures. If you use a switch to connect the failover link, use dedicated interfaces on the switch and security appliance for the failover link; do not share the interface with subinterfaces carrying regular network traffic.

On systems running in multiple context mode, the failover link resides in the system context. This interface and the state link, if used, are the only interfaces that you can configure in the system context. All other interfaces are allocated to and configured from within security contexts.

Note The IP address and MAC address for the failover link do not change at failover.

The **no** form of this command also clears the failover interface IP address configuration.

This command must be part of the configuration when bootstrapping a security appliance for LAN failover.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example configures the failover LAN interface on a PIX 500 series security appliance:

```
hostname(config)# failover lan interface folink Ethernet4
```

The following example configures the failover LAN interface using a subinterface on an ASA 5500 series adaptive security appliance (except for the ASA 5505 adaptive security appliance):

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

The following example configures the failover LAN interface on the ASA 5505 adaptive security appliance:

```
hostname(config)# failover lan interface folink Vlan6
```

Related Commands

Command	Description
failover lan enable	Enables LAN-based failover on the PIX security appliance.
failover lan unit	Specifies the LAN-based failover primary or secondary unit.
failover link	Specifies the Stateful Failover interface.

failover lan unit

To configure the security appliance as either the primary or secondary unit in a LAN failover configuration, use the **failover lan unit** command in global configuration mode. To restore the default setting, use the **no** form of this command.

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

Syntax Description

primary	Specifies the security appliance as a primary unit.
secondary	Specifies the security appliance as a secondary unit.

Defaults

Secondary.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

For Active/Standby failover, the primary and secondary designation for the failover unit refers to which unit becomes active at boot time. The primary unit becomes the active unit at boot time when the following occurs:

- The primary and secondary unit both complete their boot sequence within the first failover poll check.
- The primary unit boots before the secondary unit.

If the secondary unit is already active when the primary unit boots, the primary unit does not take control; it becomes the standby unit. In this case, you need to issue the **no failover active** command on the secondary (active) unit to force the primary unit back to active status.

For Active/Active failover, each failover group is assigned a primary or secondary unit preference. This preference determines on which unit in the failover pair the contexts in the failover group become active at startup when both units start simultaneously (within the failover polling period).

This command must be part of the configuration when bootstrapping a security appliance for LAN failover.

Examples

The following example sets the security appliance as the primary unit in LAN-based failover:

```
hostname(config)# failover lan unit primary
```

Related Commands

Command	Description
failover lan enable	Enables LAN-based failover on the PIX security appliance.
failover lan interface	Specifies the interface used for failover communication.

failover link

To specify the Stateful Failover interface, use the **failover link** command in global configuration mode. To remove the Stateful Failover interface, use the **no** form of this command.

failover link *if_name* [*phy_if*]

no failover link

Syntax Description

if_name	Specifies the name of the security appliance interface dedicated to Stateful Failover.
phy_if	(Optional) Specifies the physical or logical interface port. If the Stateful Failover interface is sharing the interface assigned for failover communication or sharing a standard firewall interface, then this argument is not required.

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 modified to include the *phy_if* argument.
7.0(4)	This command was modified to accept standard firewall interfaces.

Usage Guidelines

This command is not available on the ASA 5505 series adaptive security appliance, which does not support Stateful Failover.

The physical or logical interface argument is required when not sharing the failover communication or a standard firewall interface.

The **failover link** command enables Stateful Failover. Enter the **no failover link** command to disable Stateful Failover. If you are using a dedicated Stateful Failover interface, the **no failover link** command also clears the Stateful Failover interface IP address configuration.

To use Stateful Failover, you must configure a Stateful Failover link to pass all state information. You have three options for configuring a Stateful Failover link:

- You can use a dedicated Ethernet interface for the Stateful Failover link.
- If you are using LAN-based failover, you can share the failover link.

- You can share a regular data interface, such as the inside interface. However, this option is not recommended.

If you are using a dedicated Ethernet interface for the Stateful Failover link, you can use either a switch or a crossover cable to directly connect the units. If you use a switch, no other hosts or routers should be on this link.

Note Enable the PortFast option on Cisco switch ports that connect directly to the security appliance.

If you are using the failover link as the Stateful Failover link, you should use the fastest Ethernet interface available. If you experience performance problems on that interface, consider dedicating a separate interface for the Stateful Failover interface.

If you use a data interface as the Stateful Failover link, you will receive the following warning when you specify that interface as the Stateful Failover link:

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

Sharing a data interface with the Stateful Failover interface can leave you vulnerable to replay attacks. Additionally, large amounts of Stateful Failover traffic may be sent on the interface, causing performance problems on that network segment.

Note Using a data interface as the Stateful Failover interface is only supported in single context, routed mode.

In multiple context mode, the Stateful Failover link resides in the system context. This interface and the failover interface are the only interfaces in the system context. All other interfaces are allocated to and configured from within security contexts.

Note The IP address and MAC address for the Stateful Failover link does not change at failover unless the Stateful Failover link is configured on a regular data interface.

Caution All information sent over the failover and Stateful Failover links is sent in clear text unless you secure the communication with a failover key. If the security appliance is used to terminate VPN tunnels, this information includes any user names, passwords and preshared keys used for establishing the tunnels. Transmitting this sensitive data in clear text could pose a significant security risk. We recommend securing the failover communication with a failover key if you are using the security appliance to terminate VPN tunnels.

Examples

The following example shows how to specify a dedicated interface as the Stateful Failover interface. The interface in the example does not have an existing configuration.

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

Related Commands

Command	Description
failover interface ip	Configures the IP address of the **failover** command and stateful failover interface.
failover lan interface	Specifies the interface used for failover communication.

failover mac address

To specify the failover virtual MAC address for a physical interface, use the **failover mac address** command in global configuration mode. To remove the virtual MAC address, use the **no** form of this command.

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

Syntax Description

phy_if	The physical name of the interface to set the MAC address.
active_mac	The MAC address assigned to the specified interface the active security appliance. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.
standby_mac	The MAC address assigned to the specified interface of the standby security appliance. The MAC address must be entered in h.h.h format, where h is a 16-bit hexadecimal number.

Defaults

Not configured.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **failover mac address** command lets you configure virtual MAC addresses for an Active/Standby failover pair. If virtual MAC addresses are not defined, then when each failover unit boots it uses the burned-in MAC addresses for its interfaces and exchanges those addresses with its failover peer. The MAC addresses for the interfaces on the primary unit are used for the interfaces on the active unit.

However, if both units are not brought online at the same time and the secondary unit boots first and becomes active, it uses the burned-in MAC addresses for its own interfaces. When the primary unit comes online, the secondary unit will obtain the MAC addresses from the primary unit. This change can disrupt network traffic. Configuring virtual MAC addresses for the interfaces ensures that the secondary unit uses the correct MAC address when it is the active unit, even if it comes online before the primary unit.

The **failover mac address** command is unnecessary (and therefore cannot be used) on an interface configured for LAN-based failover because the **failover lan interface** command does not change the IP and MAC addresses when failover occurs. This command has no effect when the security appliance is configured for Active/Active failover.

When adding the **failover mac address** command to your configuration, it is best to configure the virtual MAC address, save the configuration to Flash memory, and then reload the failover pair. If the virtual MAC address is added when there are active connections, then those connections stop. Also, you must write the complete configuration, including the **failover mac address** command, to the Flash memory of the secondary security appliance for the virtual MAC addressing to take effect.

If the **failover mac address** is specified in the configuration of the primary unit, it should also be specified in the bootstrap configuration of the secondary unit.

Note This command applies to Active/Standby failover only. In Active/Active failover, you configure the virtual MAC address for each interface in a failover group with the **mac address** command in failover group configuration mode.

Examples

The following example configures the active and standby MAC addresses for the interface named intf2:

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

Related Commands

Command	Description
show interface	Displays interface status, configuration, and statistics.

failover polltime

To specify the failover unit poll and hold times, use the **failover polltime** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a unit must receive a hello message on the failover link, after which the peer unit is declared failed. Valid values are from 3 to 45 seconds or from 800 to 999 milliseconds if the optional **msec** keyword is used.
msec	(Optional) Specifies that the given time is in milliseconds.
poll_time	Amount of time between hello messages. Valid values are from 1 to 15 seconds or from 200 to 999 milliseconds if the optional **msec** keyword is used.
unit	(Optional) Indicates that the command is used for unit poll and hold times. Adding this keyword to the command does not have any affect on the command, but it can make it easier to differentiate this command from the **failover polltime interface** commands in the configuration.

Defaults

The default values on the PIX security appliance are as follows:

- The *poll_time* is 15 seconds.
- The **holdtime** *time* is 45 seconds.

The default values on the ASA security appliance are as follows:

- The *poll_time* is 1 second.
- The **holdtime** *time* is 15 seconds.

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 changed from the **failover poll** command to the **failover polltime** command and now includes **unit** and **holdtime** keywords.
7.2(1)	The **msec** keyword was added to the **holdtime** keyword. The **polltime** minimum value was reduced to 200 milliseconds from 500 milliseconds. The **holdtime** minimum value was reduced to 800 milliseconds from 3 seconds.

Usage Guidelines

You cannot enter a **holdtime** value that is less than 3 times the unit poll time. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection can cause unnecessary switch overs when the network is temporarily congested.

If a unit does not hear hello packet on the failover communication interface or cable for one polling period, additional testing occurs through the remaining interfaces. If there is still no response from the peer unit during the hold time, the unit is considered failed and, if the failed unit is the active unit, the standby unit takes over as the active unit.

You can include both **failover polltime** [**unit**] and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a security appliance in a failover configuration, you should decrease the failover hold time on the security appliance to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example changes the unit poll time frequency to 3 seconds:

```
hostname(config)# failover polltime 3
```

The following example configures the security appliance to send a hello packet every 200 milliseconds and to fail over in 800 milliseconds if no hello packets are received on the failover interface within that time. The optional **unit** keyword is included in the command.

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

Related Commands

Command	Description
failover polltime interface	Specifies the interface poll and hold times for Active/Standby failover configurations.
polltime interface	Specifies the interface poll and hold times for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover polltime interface

To specify the data interface poll and hold times in an Active/Standby failover configuration, use the **failover polltime interface** command in global configuration mode. To restore the default poll and hold times, use the **no** form of this command.

failover polltime interface [**msec**] *time* [**holdtime** *time*]

no failover polltime interface [**msec**] *time* [**holdtime** *time*]

Syntax Description

holdtime *time*	(Optional) Sets the time during which a data interface must receive a hello message on the data interface, after which the peer is declared failed. Valid values are from 5 to 75 seconds.
interface *time*	Specifies the poll time for interface monitoring. Valid values range from 1 to 15 seconds. If the optional **msec** keyword is used, the valid values are from 500 to 999 milliseconds.
msec	(Optional) Specifies that the given time is in milliseconds.

Defaults

The default values are as follows:

- The poll *time* is 5 seconds.
- The **holdtime** *time* is 5 times the poll *time*.

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 changed from the **failover poll** command to the **failover polltime** command and includes **unit**, **interface**, and **holdtime** keywords.
7.2(1)	The optional **holdtime** *time* and the ability to specify the poll time in milliseconds was added.

Usage Guidelines

Use the **failover polltime interface** command to change the frequency that hello packets are sent out on data interfaces. This command is available for Active/Standby failover only. For Active/Active failover, use the **polltime interface** command in failover group configuration mode instead of the **failover polltime interface** command.

You cannot enter a **holdtime** value that is less than 5 times the unit poll time. With a faster poll time, the security appliance can detect failure and trigger failover faster. However, faster detection can cause unnecessary switchovers when the network is temporarily congested. Interface testing begins when a hello packet is not heard on the interface for over half the hold time.

You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note When CTIQBE traffic is passed through a security appliance in a failover configuration, you should decrease the failover hold time on the security appliance to below 30 seconds. The CTIQBE keepalive timeout is 30 seconds and may time out before failover occurs in a failover situation. If CTIQBE times out, Cisco IP SoftPhone connections to Cisco CallManager are dropped, and the IP SoftPhone clients need to reregister with the CallManager.

Examples

The following example sets the interface poll time frequency to 15 seconds:

```
hostname(config)# failover polltime interface 15
```

The following example sets the interface poll time frequency to 500 milliseconds and the hold time to 5 seconds:

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

Related Commands

Command	Description
failover polltime	Specifies the unit failover poll and hold times.
polltime interface	Specifies the interface polltime for Active/Active failover configurations.
show failover	Displays failover configuration information.

failover reload-standby

To force the standby unit to reboot, use the **failover reload-standby** command in privileged EXEC mode.

failover reload-standby

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
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use this command when your failover units do not synchronize. The standby unit restarts and resynchronizes to the active unit after it finishes booting.

Examples

The following example shows how to use the **failover reload-standby** command on the active unit to force the standby unit to reboot:

```
hostname# failover reload-standby
```

Related Commands

Command	Description
write standby	Writes the running configuration to the memory on the standby unit.

failover replication http

To enable HTTP (port 80) connection replication, use the **failover replication http** command in global configuration mode. To disable HTTP connection replication, use the **no** form of this command.

failover replication http

no failover replication http

Syntax Description

This command has no arguments or keywords.

Defaults

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
Preexisting	This command was changed from **failover replicate http** to **failover replication http**.

Usage Guidelines

By default, the security appliance does not replicate HTTP session information when Stateful Failover is enabled. Because HTTP sessions are typically short-lived, and because HTTP clients typically retry failed connection attempts, not replicating HTTP sessions increases system performance without causing serious data or connection loss. The **failover replication http** command enables the stateful replication of HTTP sessions in a Stateful Failover environment, but could have a negative effect on system performance.

In Active/Active failover configurations, you control HTTP session replication per failover group using the **replication http** command in failover group configuration mode.

Examples

The following example shows how to enable HTTP connection replication:

```
hostname(config)# failover replication http
```

Related Commands

Command	Description
replication http	Enables HTTP session replication for a specific failover group.
show running-config failover	Displays the **failover** commands in the running configuration.

failover reset

To restore a failed security appliance to an unfailed state, use the **failover reset** command in privileged EXEC mode.

failover reset [**group** *group_id*]

Syntax Description

group	(Optional) Specifies a failover group. The **group** keyword applies to Active/Active failover only.
group_id	Failover group number.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified to allow the optional failover group ID.

Usage Guidelines

The **failover reset** command allows you to change the failed unit or group to an unfailed state. The **failover reset** command can be entered on either unit, but we recommend that you always enter the command on the active unit. Entering the **failover reset** command at the active unit will "unfail" the standby unit.

You can display the failover status of the unit with the **show failover** or **show failover state** commands.

There is no **no** version of this command.

In Active/Active failover, entering **failover reset** resets the whole unit. Specifying a failover group with the command resets only the specified group.

Examples

The following example shows how to change a failed unit to an unfailed state:

```
hostname# failover reset
```

Related Commands

Command	Description
failover interface-policy	Specifies the policy for failover when monitoring detects interface failures.
show failover	Displays information about the failover status of the unit.

failover timeout

To specify the failover reconnect timeout value for asymmetrically routed sessions, use the **failover timeout** command in global configuration mode. To restore the default timeout value, use the **no** form of this command.

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

Syntax Description

hh	Specifies the number of hours in the timeout value. Valid values range from -1 to 1193. By default, this value is set to 0. Setting this value to -1 disables the timeout, allowing connections to reconnect after any amount of time. Setting this value to 0, without specifying any of the other timeout values, sets the command back to the default value, which prevents connections from reconnecting. Entering **no failover timeout** command also sets this value to the default (0). **Note** When set to the default value, this command does not appear in the running configuration.
mm	(Optional) Specifies the number of minutes in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.
ss	(Optional) Specifies the number of seconds in the timeout value. Valid values range from 0 to 59. By default, this value is set to 0.

Defaults

By default, *hh*, *mm*, and *ss* are 0, which prevents connections from reconnecting.

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 modified to appear in the command listing.

Usage Guidelines

This command is used in conjunction with the **static** command with the **nailed** option. The **nailed** option allows connections to be reestablished in a specified amount of time after bootup or a system goes active. The **failover timeout** command specifies that amount of time. If not configured, the connections cannot be reestablished. The **failover timeout** command does not affect the **asr-group** command.

Note Adding the **nailed** option to the **static** command causes TCP state tracking and sequence checking to be skipped for the connection.

Enter the **no** form of this command restores the default value. Entering **failover timeout 0** also restores the default value. When set to the default value, this command does not appear in the running configuration.

Examples

The following example switches the standby group 1 to active:

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

Related Commands

Command	Description
static	Configures a persistent one-to-one address translation rule by mapping a local IP address to a global IP address.

file-bookmarks

To customize the File Bookmarks title or the File Bookmarks links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **file-bookmarks** command from webvpn customization configuration mode. To remove the command from the configuration and cause the value to be inherited, use the **no** form of this command.

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

no file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

Syntax Description

link	Specifies you are changing the links.
title	Specifies you are changing the title.
style	Specifies you are changing the HTML style.
text	Specifies you are changing the text.
value	The actual text to display (maximum 256 characters), or CSS parameters (maximum 256 characters).

Defaults

The default link style is color:#669999;border-bottom: 1px solid #669999;text-decoration:none.

The default title style is color:#669999;background-color:#99CCCC;font-weight:bold.

The default title text is “File Folder Bookmarks”.

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 customization configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid CSS parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the W3C website at www.w3.org. Appendix F of the CSS 2.1 Specification contains a convenient list of CSS parameters, and is available at www.w3.org/TR/CSS21/propidx.html.

Here are some tips for making the most common changes to the WebVPN pages—the page colors:

- 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.

Note To easily customize the WebVPN pages, we recommend that you use ASDM, which has convenient features for configuring style elements, including color swatches and preview capabilities.

Examples

The following example customizes the File Bookmarks title to "Corporate File Bookmarks":

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

Related Commands

Command	Description
application-access	Customizes the Application Access box of the WebVPN Home page.
browse-networks	Customizes the Browse Networks box of the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.
web-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.

file-browsing

To enable or disable CIFS/FTP file browsing for file servers or shares, use the **file-browsing** command in dap webvpn configuration mode.

file-browsing enable | disable

enable | disable	Enables or disables the ability to browse for file servers or shares.

Defaults

No default value or behaviors.

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**
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The following usage notes apply to file browsing:

- File browsing does not support internationalization.
- Browsing requires NBNS (Master Browser or WINS). If that fails or is not configured, we use DNS.

The security appliance can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the tunnel group
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or tunnel group.

When you enable or disable an attribute for a DAP record, the security appliance applies that value and enforces it. For example, when you disable file browsing in dap webvpn mode, the security appliance looks no further for a value. When you instead set no value for the **file-browsing** command, the attribute is not present in the DAP record, so the security appliance moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable file browsing for the DAP record called Finance:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-browsing enable
hostname(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-entry	Enables or disables the ability to enter file server names to access.

file-encoding

To specify the character encoding for pages from Common Internet File System servers, use the **file-encoding** command in webvpn configuration mode. To remove the values of the file-encoding attribute use the **no** form of this command.

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {server-name | server-ip-addr}

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets. You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper-case to lower-case in the security appliance configuration.
server-ip-addr	IP address, in dotted decimal notation, of the CIFS server for which you want to specify character encoding.
server-name	Name of the CIFS server for which you want to specify character encoding. The security appliance retains the case you specify, although it ignores the case when matching the name to a server.

Defaults

Pages from all CIFS servers that do not have explicit file-encoding entries in the WebVPN configuration inherit the character encoding value from the character-encoding attribute.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Enter file-encoding entries for all CIFS servers that require character encodings that differ from the value of the webvpn character-encoding attribute.

The WebVPN portal pages downloaded from the CIFS server to the WebVPN user encode the value of the WebVPN file-encoding attribute identifying the server, or if one does not, they inherit the value of the character-encoding attribute. The remote user's browser maps this value to an entry in its character encoding set to determine the proper character set to use. The WebVPN portal pages do not specify a

value if WebVPN configuration does not specify a file-encoding entry for the CIFS server and the character-encoding attribute is not set. The remote browser uses its own default encoding if the WebVPN portal page does not specify the character encoding or if it specifies a character encoding value that the browser does not support.

The mapping of CIFS servers to their appropriate character encoding, globally with the webvpn character-encoding attribute, and individually with file-encoding overrides, provides for the accurate handling and display of CIFS pages when the proper rendering of file names or directory paths, as well as pages, are an issue.

Note The character-encoding and file-encoding values do not exclude the font family to be used by the browser. You need to complement the setting of one these values with the **page style** command in webvpn customization command mode to replace the font family if you are using Japanese Shift_JIS character encoding, as shown in the following example, or enter the **no page style** command in webvpn customization command mode to remove the font family.

Examples

The following example sets the file-encoding attribute of the CIFS server named "CISCO-server-jp" to support Japanese Shift_JIS characters, removes the font family, and retains the default background color:

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding CISCO-server-jp shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

The following example sets the file-encoding attribute of the CIFS server 10.86.5.174 to support IBM860 (alias "CP860") characters:

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

Related Commands

Command	Description
character-encoding	Specifies the global character encoding used in all WebVPN portal pages except for pages from servers specified in file-encoding entries in the WebVPN configuration.
show running-config [all] webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.
debug webvpn cifs	Displays debug messages about the Common Internet File System.

file-entry

To enable or disable the ability of a user to enter file server names to access, use the **file-entry** command in dap webvpn configuration mode.

file-entry enable | disable

enable | disable	Enables or disables the ability to enter file server names to access.

Defaults

No default value or behaviors.

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**
Dap webvpn configuration	•	•	•	—	—

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The security appliance can apply attribute values from a variety of sources. It applies them according to the following hierarchy:

1. DAP record
2. Username
3. Group policy
4. Group policy for the Connection Profile (tunnel group)
5. Default group policy

It follows that DAP values for an attribute have a higher priority than those configured for a user, group policy, or Connection Profile.

When you enable or disable an attribute for a DAP record, the security appliance applies that value and enforces it. For example, when you disable file entry in dap webvpn mode, the security appliance looks no further for a value. When you instead set no value for the **file-entry** command, the attribute is not present in the DAP record, so the security appliance moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

The following example shows how to enable file entry for the DAP record called Finance:

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-entry enable
```

```
hostname(config-dap-webvpn)#
```

Related Commands

Command	Description
dynamic-access-policy-record	Creates a DAP record.
file-browsing	Enables or disables the ability to browse for file servers or shares.

filter

To specify the name of the access list to use for WebVPN connections for this group policy or username, use the **filter** command in webvpn configuration mode. To remove the access list, including a null value created by issuing the **filter none** command, use the **no** form of this command.

filter {**value** *ACLname* | **none**}

no filter

Syntax Description

none	Indicates that there is no **webvpntype** access list. Sets a null value, thereby disallowing an access list. Prevents inheriting an access list from another group policy.
value *ACLname*	Provides the name of the previously configured access list.

Defaults

WebVPN access lists do not apply until you use the **filter** command to specify them.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **no** option allows inheritance of a value from another group policy. To prevent inheriting filter values, use the **filter value none** command.

You configure ACLs to permit or deny various types of traffic for this user or group policy. You then use the **filter** command to apply those ACLs for WebVPN traffic.

WebVPN does not use ACLs defined in the **vpn-filter** command.

Examples

The following example shows how to set a filter that invokes an access list named *acl_in* for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
```

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

filter activex

To remove ActiveX objects in HTTP traffic passing through the security appliance, use the **filter activex** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter activex | java **<***port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

no filter activex | java **<***port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 21, but other values are accepted. The **http** or **url** literal can be used for port 21. The range of values permitted is 0 to 65535. For a listing of the well-known ports and their literal values, see
-*port*	(Optional) Specifies a port range.
except	Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

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
Preexisting	This command was preexisting.

Usage Guidelines

ActiveX objects may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can disable ActiveX objects with the **filter activex** command.

ActiveX controls, formerly known as OLE or OCX controls, are components you can insert in a web page or other application. These controls include custom forms, calendars, or any of the extensive third-party forms for gathering or displaying information. As a technology, ActiveX creates many potential problems for network clients including causing workstations to fail, introducing network security problems, or being used to attack servers.

The **filter activex** command command blocks the HTML <object> commands by commenting them out within the HTML web page. ActiveX filtering of HTML files is performed by selectively replacing the <APPLET> and </APPLET> and <OBJECT CLASSID> and </OBJECT> tags with comments. Filtering of nested tags is supported by converting top-level tags to comments.

Caution The <object> tag is also used for Java applets, image files, and multimedia objects, which will also be blocked by this command.

If the <object> or </object> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the security appliance cannot block the tag.

ActiveX blocking does not occur when users access an IP address referenced by the **alias** command or for WebVPN traffic.

Examples

The following example specifies that Activex objects are blocked on all outbound connections:

```
hostname(config)# filter activex 80 0 0 0 0
```

This command specifies that the ActiveX object blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

Related Commands\

Commands	Description
filter url	Directs traffic to a URL filtering server.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies anN2H2 or Websense server for use with the **filter** command.

filter ftp

To identify the FTP traffic to be filtered by a Websense or N2H2 server, use the **filter ftp** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter ftp <*port*> [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

no filter ftp <*port*> [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 21, but other values are accepted. The **ftp** literal can be used for port 80.
-*port*	(Optional) Specifies a port range.
except	Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
allow	(Optional) When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the security appliance stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back on line.
interact-block	(Optional) Prevents users from connecting to the FTP server through an interactive FTP program.

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
Preexisting	This command was preexisting.

Usage Guidelines

The **filter ftp** command lets you identify the FTP traffic to be filtered by a Websense or N2H2 server.

After enabling this feature, when a user issues an FTP GET request to a server, the security appliance sends the request to the FTP server and to the Websense or N2H2 server at the same time. If the Websense or N2H2 server permits the connection, the security appliance allows the successful FTP return code to reach the user unchanged. For example, a successful return code is "250: CWD command successful."

If the Websense or N2H2 server denies the connection, the security appliance alters the FTP return code to show that the connection was denied. For example, the security appliance would change code 250 to "550 Requested file is prohibited by URL filtering policy." Websense only filters FTP GET commands and not PUT commands).

Use the **interactive-block** option to prevent interactive FTP sessions that do not provide the entire directory path. An interactive FTP client allows the user to change directories without typing the entire path. For example, the user might enter **cd ./files** instead of **cd /public/files**. You must identify and enable the URL filtering server before using these commands.

Examples

The following example shows how to enable FTP filtering:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
filter https	Identifies the HTTPS traffic to be filtered by a Websense sor N2H2 erver.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

filter https

To identify the HTTPS traffic to be filtered by a N2H2 or Websense server, use the **filter https** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter https <*port*> [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

no filter https <*port*> [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 443, but other values are accepted. The **https** literal can be used for port 443.
-*port*	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
allow	(Optional) When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the security appliance stops outbound port 443 traffic until the N2H2 or Websense server is back on line.

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
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance supports filtering of HTTPS and FTP sites using an external Websense or N2H2 filtering server.

HTTPS filtering works by preventing the completion of SSL connection negotiation if the site is not allowed. The browser displays an error message such as "The Page or the content cannot be displayed."

Because HTTPS content is encrypted, the security appliance sends the URL lookup without directory and filename information.

Examples

The following example filters all outbound HTTPS connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

filter java

To remove Java applets from HTTP traffic passing through the security appliance, use the **filter java** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

Syntax Description

port	The TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The **http** or **url** literal can be used for port 80.
*port***-***port*	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous **filter** condition.
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
local_mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.

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
Preexisting	This command was preexisting.

Usage Guidelines

Java applets may pose security risks because they can contain code intended to attack hosts and servers on a protected network. You can remove Java applets with the **filter java** command.

The **filter java** command filters out Java applets that return to the security appliance from an outbound connection. The user still receives the HTML page, but the web page source for the applet is commented out so that the applet cannot execute. The **filter java** command does not filter WebVPN traffic.

If the applet or /applet HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the security appliance cannot block the tag. If Java applets are known to be in <object> tags, use the **filter activex** command to remove them.

Examples

The following example specifies that Java applets are blocked on all outbound connections:

```
hostname(config)# filter java 80 0 0 0 0
```

This command specifies that the Java applet blocking applies to web traffic on port 80 from any local host and for connections to any foreign host.

The following example blocks downloading of Java applets to a host on a protected network:

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

This command prevents host 192.168.3.3 from downloading Java applets.

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

filter url

To direct traffic to a URL filtering server, use the **filter url** command in global configuration mode. To remove the configuration, use the **no** form of this command.

filter url <*port*> [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url <*port*> [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

Syntax Description

allow	When the server is unavailable, let outbound connections pass through the security appliance without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the security appliance stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back on line.
cgi_truncate	When a URL has a parameter list starting with a question mark (?), such as a CGI script, truncate the URL sent to the filtering server by removing all characters after and including the question mark.
except	Creates an exception to a previous **filter** condition.
foreign_ip	The IP address of the lowest security level interface to which access is sought. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
foreign_mask	Network mask of *foreign_ip*. Always specify a specific mask value. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
http	Specifies port 80. You can enter **http** or **www** instead of 80 to specify port 80.)
local_ip	The IP address of the highest security level interface from which access is sought. You can set this address to **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
local_mask	Network mask of *local_ip*. You can use **0.0.0.0** (or in shortened form, **0**) to specify all hosts.
longurl-deny	Denies the URL request if the URL is over the URL buffer size limit or the URL buffer is not available.
longurl-truncate	Sends only the originating hostname or IP address to the N2H2 or Websense server if the URL is over the URL buffer limit.
mask	Any mask.
-*port*	(Optional) The TCP port to which filtering is applied. Typically, this is port 80, but other values are accepted. The **http** or **url** literal can be used for port 80. Adding a second port after a hyphen optionally identifies a range of ports.
proxy-block	Prevents users from connecting to an HTTP proxy server.
url	Filter URLs from data moving through the security appliance.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The **filter url** command lets you prevent outbound users from accessing World Wide Web URLs that you designate using the N2H2 or Websense filtering application.

Note The **url-server** command must be configured before issuing the **filter url** command.

The **allow** option to the **filter url** command determines how the security appliance behaves if the N2H2 or Websense server goes off line. If you use the **allow** option with the **filter url** command and the N2H2 or Websense server goes offline, port 80 traffic passes through the security appliance without filtering. Used without the **allow** option and with the server off line, the security appliance stops outbound port 80 (Web) traffic until the server is back on line, or if another URL server is available, passes control to the next URL server.

Note With the **allow** option set, the security appliance now passes control to an alternate server if the N2H2 or Websense server goes off line.

The N2H2 or Websense server works with the security appliance to deny users from access to websites based on the company security policy.

Using the Filtering Server

Websense protocol Version 4 enables group and username authentication between a host and a security appliance. The security appliance performs a username lookup, and then Websense server handles URL filtering and username logging.

The N2H2 server must be a Windows workstation (2000, NT, or XP), running an IFP Server, with a recommended minimum of 512 MB of RAM. Also, the long URL support for the N2H2 service is capped at 3 KB, less than the cap for Websense.

Websense protocol Version 4 contains the following enhancements:

- URL filtering allows the security appliance to check outgoing URL requests against the policy defined on the Websense server.
- Username logging tracks username, group, and domain name on the Websense server.
- Username lookup enables the security appliance to use the user authentication table to map the host's IP address to the username.

Information on Websense is available at the following website:

http://www.websense.com/

Configuration Procedure

Follow these steps to filter URLs:

Step 1 Designate an N2H2 or Websense server with the appropriate vendor-specific form of the **url-server** command.

Step 2 Enable filtering with the **filter** command.

Step 3 If needed, improve throughput with the **url-cache** command. However, this command does not update Websense logs, which may affect Websense accounting reports. Accumulate Websense run logs before using the **url-cache** command.

Step 4 Use the **show url-cache statistics** and the **show perfmon** commands to view run information.

Working with Long URLs

Filtering URLs up to 4 KB is supported for the Websense filtering server, and up to 3 KB for the N2H2 filtering server.

Use the **longurl-truncate** and **cgi-truncate** options to allow handling of URL requests longer than the maximum permitted size.

If a URL is longer than the maximum, and you do not enable the **longurl-truncate** or **longurl-deny** options, the security appliance drops the packet.

The **longurl-truncate** option causes the security appliance to send only the hostname or IP address portion of the URL for evaluation to the filtering server when the URL is longer than the maximum length permitted. Use the **longurl-deny** option to deny outbound URL traffic if the URL is longer than the maximum permitted.

Use the **cgi-truncate** option to truncate CGI URLs to include only the CGI script location and the script name without any parameters. Many long HTTP requests are CGI requests. If the parameters list is very long, waiting and sending the complete CGI request including the parameter list can use up memory resources and affect security appliance performance.

Buffering HTTP Responses

By default, when a user issues a request to connect to a specific website, the security appliance sends the request to the web server and to the filtering server at the same time. If the filtering server does not respond before the web content server, the response from the web server is dropped. This delays the web server response from the point of view of the web client.

By enabling the HTTP response buffer, replies from web content servers are buffered and the responses will be forwarded to the requesting user if the filtering server allows the connection. This prevents the delay that may otherwise occur.

To enable the HTTP response buffer, enter the following command:

```
url-block block block-buffer-limit
```

Replace *block-buffer* with the maximum number of blocks that will be buffered. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks that can be buffered at one time.

Examples

The following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

The following example blocks all outbound HTTP connections destined to a proxy server that listens on port 8080:

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the security appliance.
filter java	Removes Java applets from HTTP traffic passing through the security appliance.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

fips enable

To enable policy-checking to enforce FIPS compliance on the system or module, use the **fips enable** commandin global configuration mode. To disable policy-checkin, use the **no** form of this command.

fips enable

no fips enable

Syntax Description

enable	Enables or disables policy-checking to enforce FIPS compliance.

Defaults

This command has no default settings.

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(4)	This command was introduced.

Usage Guidelines

To run in a FIPS-compliant mode of operation, you must apply both the **fips enable** command and the proper configuration specified in the Security Policy. The internal API allows the device to migrate towards enforcing proper configuration at run-time.

When “fips enable” is present in the startup-configuration, FIPS POST will run and print the following console message:

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
```

```
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

Examples

The following shows policy-checking to enforce FIPS compliance on the system:

```
sw8-ASA(config)# fips enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

fips self-test poweron

To execute power-on self-tests, use the **fips self-test powereon** commandin privileged EXEC mode.

fips self-test poweron

Syntax Description

poweron	Executes Power-On Self-Tests.

Defaults

This command has no default settings.

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(4)	This command was introduced.

Usage Guidelines

Executing this command causes the device to run all self-tests required for FIPS 140-2 compliance. Tests are compreised of: cryptographic algorithm test, software integrity test and critical functions test.

Examples

The following example shows the system executing the power-on of self-tests:

```
sw8-5520(config)# fips self-test poweron
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to Flash.
fips enable	Enables or disablea policy-checking to enforce FIPS compliance on the system or module.
show crashinfo console	Reads, writes, and configures crash write to Flash.
show running-config fips	Displays the FIPS configuration that is running on the security appliance.

firewall transparent

To set the firewall mode to transparent mode, use the **firewall transparent** command in global configuration mode. To restore routed mode, use the **no** form of this command. A transparent firewall is a Layer 2 firewall that acts like a "bump in the wire," or a "stealth firewall," and is not seen as a router hop to connected devices.

firewall transparent

no firewall transparent

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.

Usage Guidelines

For multiple context mode, you can use only one firewall mode for all contexts. You must set the mode in the system configuration. This command also appears in each context configuration for informational purposes only; you cannot enter this command in a context.

When you change modes, the security appliance clears the configuration because many commands are not supported for both modes. If you already have a populated configuration, be sure to back up your configuration before changing the mode; you can use this backup for reference when creating your new configuration.

If you download a text configuration to the security appliance that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the security appliance changes the mode as soon as it reads the command and then continues reading the configuration you downloaded. If the command is later in the configuration, the security appliance clears all the preceding lines in the configuration.

Examples

The following example changes the firewall mode to transparent:

```
hostname(config)# firewall transparent
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show firewall	Shows the firewall mode.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

flowcontrol

To enable pause (XOFF) frames for flow control on 10 Gigabit Ethernet interfaces only, use the **flowcontrol** command in interface configuration mode. To disable pause frames, use the **no** form of this command.

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

Syntax Description

low_water	Sets the low-water mark, between 0 and 511 KB. After the network interface controller (NIC) sends a pause frame, when the buffer usage is reduced below the low-water mark, the NIC sends an XON frame. The link partner can resume traffic after receiving an XON frame. The default is 64 KB.
pause_time	Sets the pause refresh threshold value, between 0 and 65535. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by this timer value in the pause frame. If the buffer usage is consistently above the high-water mark, pause frames are sent repeatedly, controlled by the pause refresh threshold value. The default is 26624.
noconfirm	Applies the command without confirmation. Because this command resets the interface, without this option, you are asked to confirm the configuration change.
high_water	Sets the high-water mark, between 0 and 511 KB. When the buffer usage exceeds the high-water mark, the NIC sends a pause frame. The default is 128 KB.

This command has no arguments or keywords.

Command Default

Pause frames are disabled by default.

The default high watermark is 128 KB.

The default low watermark is 64 KB.

The default pause refresh threshold value is 26664.

Command Modes

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

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

Command History

Release	Modification
8.2(2)	This command was introduced.

Usage Guidelines

Enter this command for a physical interface.

If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue.

When you enable this command, pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage:

1. The NIC sends a pause frame when the buffer usage exceeds the high-water mark.
2. After a pause is sent, the NIC sends an XON frame when the buffer usage is reduced below the low-water mark.
3. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame.
4. If the buffer usage is consistently above the high-water mark, the NIC sends pause frames repeatedly, controlled by the pause refresh threshold value.

When you use this command, you see the following warning:

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

To change the parameters without being prompted, use the **noconfirm** keyword.

Note Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Examples

The following example enables pause frames using the default settings:

```
hostname(config)# interface tengigabitethernet 1/0
hostname(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
hostname(config-if)# y
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

format

To erase all files and format the file system, use the **format** command in privileged EXEC mode. This command erases all files on the file system, including hidden system files, and reinstalls the file system.

format {**disk0: | disk1: | flash:**}

Syntax Description

disk0*:*	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

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
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **format** command erases all data on the specified file system and then rewrites the FAT information to the device.

Caution Use the **format** command with extreme caution, only when necessary to clean up corrupted Flash memory.

To delete all visible files (excluding hidden system files), enter the **delete /recursive** command, instead of the **format** command.

Note On Cisco PIX security appliances, the **erase** and **format** commands do the same thing, destroy user data with the 0xFF pattern.

To repair a corrupt file system, try entering the **fsck** command before entering the **format** command.

Note On Cisco ASA 5500 series security appliances, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information.

To repair a corrupt file system, try entering the **fsck** command before entering the **format** command.

Examples

This example shows how to format the Flash memory:

```
hostname# format flash:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the Flash memory.
fsck	Repairs a corrupt file system.

forward interface

For models with a built-in switch, such as the ASA 5505 adaptive security appliance, use the **forward interface** command in interface configuration mode to restore connectivity for one VLAN from initiating contact to one other VLAN. To restrict one VLAN from initiating contact to one other VLAN, use the **no** form of this command. You might need to restrict one VLAN depending on how many VLANs your license supports.

forward interface vlan *number*

no forward interface vlan *number*

Syntax Description

vlan *number*	Specifies the VLAN ID to which this VLAN interface cannot initiate traffic.

Defaults

By default, all interfaces can initiate traffic to all other 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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

In routed mode, you can configure up to three active VLANs with the ASA 5505 adaptive security appliance Base license, and up to five active VLANs with the Security Plus license. An active VLAN is a VLAN with a **nameif** command configured. You can configure up to five inactive VLANs on the ASA 5505 adaptive security appliance for either license, but if you make them active, be sure to follow the guidelines for your license.

With the Base license, the third VLAN must be configured with the **no forward interface** command to restrict this VLAN from initiating contact to one other VLAN.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside work network, and a third VLAN assigned to your home network. The home network does not need to access the work network, so you can use the **no forward interface** command on the home VLAN; the work network can access the home network, but the home network cannot access the work network.

If you already have two VLAN interfaces configured with a **nameif** command, be sure to enter the **no forward interface** command before the **nameif** command on the third interface; the security appliance does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505 adaptive security appliance.

Examples

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work interface.

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

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
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 vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

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

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

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

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

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

...
```

Related Commands

Command	Description
backup interface	Assigns an interface to be a backup link to an ISP, for example.
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
switchport access vlan	Assigns a switch port to a VLAN.

fqdn

To include the indicated FQDN in the Subject Alternative Name extension of the certificate during enrollment, use the **fqdn** command in crypto ca trustpoint configuration mode. To restore the default setting of the fqdn, use the **no** form of the command.

fqdn [*fqdn* | **none**]

no fqdn

Syntax Description

fqdn	Specifies the fully qualified domain name. The maximum length of *fqdn* is 64 characters.
none	Specifies no fully qualified domain name.

Defaults

The default setting does not include the FQDN.

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	This command was introduced.

Usage Guidelines

If you are configuring the security appliance to support authentication of a Nokia VPN Client using certificates, use the **none** keyword. See the **crypto isakmp identity** or **isakmp identity** command for more information on supporting certificate authentication of the Nokia VPN Client.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the FQDN engineering in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# fqdn engineering
hostname(config-ca-trustpoint)#
```

Related Commands

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

Command	Description
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut and paste enrollment with this trustpoint.

fragment

To provide additional management of packet fragmentation and improve compatibility with NFS, use the **fragment** command in global configuration mode. To return to the default values, use the **no** form of this command.

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

Syntax Description

chain *limit*	Specifies the maximum number of fragments into which a full IP packet can be fragmented.
interface	(Optional) Specifies the security appliance interface. If an interface is not specified, the command applies to all interfaces.
size *limit*	Sets the maximum number of fragments that can be in the IP reassembly database waiting for reassembly. **Note** The security appliance does not accept any fragments that are not part of an existing fabric chain after the queue size reaches 2/3 full. The remaining 1/3 of the queue is used to accept fragments where the source/destination IP addresses and IP identification number are the same as an incomplete fragment chain that is already partially queued. This limit is a DoS protection mechanism to help legitimate fragment chains be reassembled when there is a fragment flooding attack.
timeout *limit*	Specifies the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded.

Defaults

The defaults are as follows:

- **chain** is 24 packets
- *interface* is all interfaces
- **size** is 200
- **timeout** is 5 seconds

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 modified so that you now must choose one of the following arguments: **chain**, **size**, or **timeout**. You can no longer enter the **fragment** command without entering one of these arguments, as was supported in prior releases of the software.

Usage Guidelines

By default, the security appliance accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the security appliance to prevent fragmented packets from traversing the security appliance by entering the **fragment chain 1** *interface* command on each interface. Setting the limit to 1 means that all packets must be whole; that is, unfragmented.

If a large percentage of the network traffic through the security appliance is NFS, additional tuning might be necessary to avoid database overflow.

In an environment where the MTU size is small between the NFS server and client, such as a WAN interface, the **chain** keyword might require additional tuning. In this case, we recommend using NFS over TCP to improve efficiency.

Setting the **size** *limit* to a large value can make the security appliance more vulnerable to a DoS attack by fragment flooding. Do not set the **size** *limit* equal to or greater than the total number of blocks in the 1550 or 16384 pool.

The default values will limit DoS attacks caused by fragment flooding.

Examples

The following example shows how to prevent fragmented packets on the outside and inside interfaces:

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

Continue entering the **fragment chain 1** *interface* command for each additional interface on which you want to prevent fragmented packets.

The following example shows how to configure the fragment database on the outside interface to a maximum size of 2000, a maximum chain length of 45, and a wait time of 10 seconds:

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

frequency

To set the rate at which the selected SLA operation repeats, use the **frequency** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

frequency *seconds*

no frequency

Syntax Description

seconds	The number of seconds between SLA probes. Valid values are from 1 to 604800 seconds. This value cannot be less than the **timeout** value.

Defaults

The default frequency is 60 seconds.

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
SLA monitor protocol configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

An SLA operation repeats at a given frequency for the lifetime of the operation. For example, an **ipIcmpEcho** operation with a frequency of 60 seconds repeats by sending the echo request packets once every 60 seconds for the lifetime of the operation. For example, the default number of packets in an echo operation is 1. This packet is sent when the operation is started and is then sent again 60 seconds later.

If an individual SLA operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is increased rather than immediately repeating the operation.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 3 seconds, and the timeout value us set to 1000 milliseconds.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
```

```
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time the SLA operation waits for a response.

fsck

To perform a file system check and to repair corruptions, use the **fsck** command in privileged EXEC mode.

fsck [/no confirm]{disk0: | disk1: | flash:}

Syntax Description

/noconfirm	Optional. Do not prompt for confirmation to repair.
disk0*:*	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

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**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
7.0	This command was introduced.

Usage Guidelines

The **fsck** command checks and attempts to repair corrupt file systems. Try using this command before resorting to more permanent procedures.

The **/noconfirm** keyword automatically repairs corruptions without seeking your confirmation first.

Examples

This example shows how to check the file system of the Flash memory:

```
hostname# fsck flash:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the Flash memory.
format	Erases all files on a file system, including hidden system files, and reinstalls the file system.

ftp mode passive

To set the FTP mode to passive, use the **ftp mode passive** command in global configuration mode. To reset the FTP client to active mode, use the **no** form of this command.

ftp mode passive

no ftp mode passive

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	This command was introduced.

Usage Guidelines

The **ftp mode passive** command sets the FTP mode to passive.The security appliance can use FTP to upload or download image files or configuration files to or from an FTP server. The **ftp mode passive** command controls how the FTP client on the security appliance interacts with the FTP server.

In passive FTP, the client initiates both the control connection and the data connection. Passive mode refers to the server state, in that the server is passively accepting both the control connection and the data connection, which are initiated by the client.

In passive mode, both destination and source ports are ephemeral ports (greater than 1023). The mode is set by the client, as the client issues the **passive** command to initiate the setup of the passive data connection. The server, which is the recipient of the data connection in passive mode, responds with the port number to which it is listening for the specific connection.

Examples

The following example sets the FTP mode to passive:

```
hostname(config)# ftp mode passive
```

Related Commands

copy	Uploads or downloads image files or configuration files to or from an FTP server.

debug ftp client	Displays detailed information about FTP client activity.
show running-config ftp mode	Displays FTP client configuration.

functions (removed)

You cannot use **functions** command for Release 8.0(2). It is deprecated, and remains in this Command Reference only for reasons of backward compatibility. Use the import and export commands to create URL lists for websites, file access, and plug-ins, customizatioin, and language translations.

To configure automatic downloading of the port forwarding java applet, Citrix support, file access, file browsing, file server entry, application of a webtype ACL, HTTP Proxy, port forwarding, or URL entry over WebVPN for this user or group policy, use the **functions** command in webvpn configuration mode. To remove a configured function, use the **no** form of this command.

functions {**auto-download | citrix | file-access | file-browsing | file-entry | filter | http-proxy | url-entry | port-forward | none**}

no functions [**auto-download | citrix | file-access | file-browsing | file-entry | filter | url-entry | port-forward**]

Syntax Description

auto-download	Enables or disables automatic download of the port forwarding java applet upon WebVPN login. You must first enable port forwarding, Outlook/Exchange proxy, or HTTP proxy.
citrix	Enables or disables support for terminal services from a MetaFrame Application Server to the remote user. This keyword lets the security appliance act as a secure gateway within a secure Citrix configuration. These services provide users with access to MetaFrame applications through a standard Web browser.
file-access	Enables or disables file access. When enabled, the WebVPN home page lists file servers in the server list. You must enable file access to enable file browsing and/or file entry.
file-browsing	Enables or disables browsing for file servers and shares. You must enable file browsing to allow user entry of a file server.
file-entry	Enables or disables user ability to enter names of file servers.
filter	Applies a webtype ACL. When enabled, the security appliance applies the webtype ACL defined with the webvpn **filter** command.
http-proxy	Enables or disables the forwarding of an HTTP applet proxy to the remote user. The proxy is useful for technologies that interfere with proper mangling, such as Java, ActiveX, and Flash. It bypasses mangling while ensuring the continued use of the security appliance. The forwarded proxy modifies the browser's old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.
none	Sets a null value for all WebVPN **functions**. Prevents inheriting functions from a default or specified group policy.

port-forward	Enables port forwarding. When enabled, the security appliance uses the port forwarding list defined with the webvpn **port-forward** command.
url-entry	Enables or disables user entry of URLs. When enabled, the security appliance still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the security appliance restricts WebVPN users to the URLs on the home page.

Defaults

Functions are 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**
Webvpn configuration	•	—	•	—	—

Command History

Release	Modification
8.0(2)	This command was deprecated.
7.1(1)	The auto-download and citrix keywords were added.
7.0(1)	This command was introduced.

Usage Guidelines

To remove all configured functions, including a null value created by issuing the **functions none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting function values, use the **functions none** command.

Examples

The following example shows how to configure file access and file browsing for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.