CHAPTER 12

email through functions Commands

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 the 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(1)	This command was introduced.

Examples

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

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# email jjh@nhf.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.

Defaults

Enters privilege level 15 unless you are using command authorization, 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.

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.

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)(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 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 up to 16 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*.

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.

enforcenextupdate

To specify how to handle the NextUpdate CRL field, use the **enforcenextupdate** command in ca-crl configuration mode. 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.

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
CRL configuration	•	•	•	•	•

Command History

Release	Modification
7.0(1)	This command was introduced.

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 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(1)	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(1)	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(1)	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(1)	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.

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 [**flash:**]

Syntax Description

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.

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(1)	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.

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.

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 dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dport* [*sport*] [**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.
dport	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.
sport	(Optional) Specifies the source port to use for the established connection lookup.

Defaults

The defaults are as follows:

- *dport*—0 (wildcard)
- *sport*—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.

The following 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 0 4000
```

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 0 6000 to tcp 6000 from 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 *sport* field as 0 (wildcard). The *dport* 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.

Examples

This example shows a connection between two hosts using protocol A from the SRC port B destined for 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
```

This example shows how a connection is started by an internal host to an external host using TCP source port 6060 and any destination port. The security appliance permits return traffic between the hosts through TCP destination port 6061 and TCP source port 6059.

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 6059
```

This 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 0 6060 permitto tcp 6061 permitfrom tcp 1024-65535
```

This example shows how a local host 10.1.1.1 starts a TCP connection on port 9999 to a foreign host 209.165.201.1. The example allows packets from the foreign host 209.165.201.1 on port 4242 back to local host 10.1.1.1 on port 5454.

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

This example shows how to allow packets from foreign host 209.165.201.1 on any port back to local host 10.1.1.1 on port 5454:

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

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 exceedx 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.
drop	Drops packets that exceed the MSS.

Defaults

Packets are dropped by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **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 allows flows on port 21 to send packets in excess of MSS:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss allow
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.
help	Shows syntax help for the **policy-map**, **class**, and **description** commands.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
set connection	Configures connection values.
tcp-map	Creates a TCP map and allows access to tcp-map configuration mode.

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 mode. To reset the expiry time to a new value, use the command again. To remove the expiration time from the configuration and reset it to the default value, one minute, enter the **no** version of the 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 mode	•	—	•	—	—

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 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.

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.

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 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:

Command Mode	Firewall Mode		Security Context		
				Multiple	
	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

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 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 will mark itself as failed and a failover may 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)(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*

no failover lan interface *if_name phy_if*

Syntax Description

if_name	Specifies the name of the security appliance interface dedicated to failover.
phy_if	Specifies the physical or logical interface port.

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 modified to include the *phy_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.

Examples

The following example configures the failover LAN interface:

```
hostname(config)# failover lan interface folink e4
```

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

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

Usage Guidelines

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.

In multiple context mode, the Stateful Failover interface 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.
mtu	Specifies the maximum transmission unit for an interface.

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

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

failover polltime interface *time*

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

no failover polltime interface *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 range from 3 to 45 seconds.
interface *time*	Specifies the poll time for interface monitoring. Valid values range from 3 to 15 seconds.
msec	(Optional) Specifies that the time interval between messages is in milliseconds. Valid values are from 500 to 999 milliseconds.
time	Amount of time between hello messages. The maximum value is 15 seconds.
unit	(Optional) Sets how often hello messages are sent on the failover link.

Defaults

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

- The **unit** poll *time* is 15 seconds.
- The **holdtime** *time* is 45 seconds.
- The **interface** poll *time* is 15 seconds.

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

- The **unit** poll *time* is 1 second.
- The **holdtime** *time* is 15 seconds.
- The **interface** poll *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**, **interface**, and **holdtime** keywords.

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 switchovers when the network is temporarily congested.

When the **unit** or **interface** keywords are not specified, the poll time configured is for the unit. You can include both **failover polltime unit** and **failover polltime interface** commands in the configuration.

Note The **failover polltime interface** command applies to 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.

If a hello packet is not heard on the failover communication interface or cable during the hold time, the standby unit switches to active and the peer is considered failed. Five missed consecutive *interface* hello packets cause interface testing.

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 will need to reregister with the CallManager.

Examples

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

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

Related Commands

Command	Description
polltime interface	Specify 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.
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 mode:

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

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

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

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 Cascading Style Sheet (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	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The **style** option is expressed as any valid Cascading Style Sheet (CSS) parameters. Describing these parameters is beyond the scope of this document. For more information about CSS parameters, consult CSS specifications at the World Wide Web Consortium (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-encoding

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

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.

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 mode. To remove the access list, including a null value created by issuing the **filter none** command, use the **no** form of this command. 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.

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 mode	•	•	—	—	•

Command History

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

Usage Guidelines

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

no filter activex {[*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 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***-***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.
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

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.

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-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 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 local_mask foreign_ip foreign_mask*] [**allow**] [**interact-block**]

no filter ftp {[*port*[**-***port*] | **except** } *local_ip local_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***-***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.
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.
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 server. FTP filtering is not supported on N2H2 servers.

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 server at the same time. If the Websense 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 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 server.
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-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 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 local_mask foreign_ip foreign_mask*] [**allow**]

no filter https {[*port*[**-***port*] | **except** } *local_ip local_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***-***port*	(Optional) Specifies a port range.
except	(Optional) Creates an exception to a previous **filter** condition.
dest-port	The destination port number.
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.
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 filtering server.

Note HTTPS is not supported for the 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-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.

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 local_mask foreign_ip foreign_mask*] [**allow**] [**cgi-truncate**] [**longurl-truncate | longurl-deny**] [**proxy-block**]

no filter url {[*port*[**-***port*] | **except** } *local_ip local_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 Websense server if the URL is over the URL buffer limit.
mask	Any mask.
[*port*[**-***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		
				Multiple	
	Routed	Transparent	Single	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 Websense 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 1159 bytes 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-limit* with the maximum number of blocks that will be buffered. The permitted values are from 0 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 or disable policy-checking to enforce FIPS compliance on the system or module, use the **fips enable** command, or [**no**] **fips enable** 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

```
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** command.

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

```
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.

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 {**flash:**}

Syntax Description

flash:	Specifies the internal Flash memory, followed by a colon.

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(1)	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.

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.

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*

no fqdn

Syntax Description

fqdn	Specifies the fully qualified domain name. The maximum length of *fqdn* is 64 characters.

Defaults

The default setting is not to 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(1)	This command was introduced.

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(ca-trustpoint)# fqdn engineering
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 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.

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

Syntax Description

chain *limit*	Specifies the maximum number of packets 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 packets 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

This 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.

This 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.

ftp-map

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

ftp-map *map_name*

no ftp-map *map_name*

Syntax Description

map_name	The name of the FTP map.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **ftp-map** command to identify a specific map to use for defining the parameters for strict FTP inspection. When you enter this command, the system enters the FTP map configuration mode, which lets you enter the different commands used for defining the specific map. Use the **request-command deny** command to prevent the FTP client from sending specific commands to the FTP server.

After defining the FTP map, use the **inspect ftp strict** command to enable the map. Then use the **class-map**, **policy-map**, and **service-policy** commands to define a class of traffic, to apply the **inspect** command to the class, and to apply the policy to one or more interfaces.

Examples

The following example shows how to identify FTP traffic, define an FTP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# exit
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
hostname(config-pmap-c)# exit
```

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

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect ftp	Applies a specific FTP map to use for application inspection.
mask-syst-reply	Hides the FTP server response from clients.
policy-map	Associates a class map with specific security actions.
request-command deny	Specifies FTP commands to disallow.

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(1)	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

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, MAPI Proxy, port forwarding, or URL entry over WebVPN for this user or group policy, use the **functions** command in webvpn mode, which you enter from group-policy or username mode. To remove a configured function, use the **no** form of this command.

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.

functions {**auto-download | citrix | file-access | file-browsing | file-entry | filter | http-proxy | url-entry | mapi | port-forward | none**}

no functions [**auto-download | citrix | file-access | file-browsing | file-entry | filter | url-entry | mapi | 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.
mapi	Enables or disables Microsoft Outlook/Exchange port forwarding.
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 mode	•	—	•	—	—

Command History

Release	Modification
7.1(1)	The auto-download and citrix keywords were added.
7.0(1)	This command was introduced.

Examples

The following example shows how to configure file access, file browsing, and MAPI Proxy 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 MAPI
```

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.