

fe – fz

- feature, on page 3
- fec, on page 6
- file-bookmarks, on page 8
- file-browsing, on page 10
- file-encoding, on page 12
- file-entry, on page 14
- filter, on page 16
- filter activex, on page 18
- filter ftp, on page 20
- filter https, on page 22
- filter java, on page 24
- filter url, on page 26
- fips enable, on page 30
- fips self-test poweron, on page 32
- firewall transparent, on page 33
- flow-export active refresh-interval, on page 35
- flow-export delay flow-create, on page 37
- flow-export destination, on page 39
- flow-export event-type destination, on page 41
- flow-export template timeout-rate, on page 43
- flow-offload cluster-redirect, on page 45
- flow-offload enable, on page 46
- flow-offload-dtls, on page 49
- flow-offload-dtls, on page 51
- flow-offload-dtls egress-optimization, on page 53
- flow-offload-ipsec, on page 55
- flowcontrol, on page 57
- flow-mobility lisp, on page 60
- force re-authentication, on page 62
- format, on page 63
- forward interface, on page 65
- forward-reference (Deprecated), on page 67
- fqdn (crypto ca trustpoint), on page 69

- fqdn (network object), on page 71
- fragment, on page 73
- frequency, on page 76
- fsck, on page 78
- ftp mode passive, on page 80
- functions (Deprecated), on page 81
- fxos mode appliance, on page 83
- fxos permit, on page 85
- fxos port, on page 87

feature

To request smart licensing feature entitlements, use the **feature** command in license smart configuration mode. To remove the feature, use the **no** form of this command.

Note This command is supported on the ASA Virtual and chassis only.

feature { **tier standard** | **strong-encryption** | **context** *number* | **mobile-sp** | **carrier** }
no feature { **tier standard** | **strong-encryption** | **context** *number* | **mobile-sp** | **carrier** }

Syntax Description

carrier	Requests the Carrier (GTP/GPRS, Diameter, SCTP, M3UA) license. This license replaces the Mobile SP license.
context *number*	(Chassis only) Requests the Security Context license. Subtract the default number of contexts contained in the standard license. For example, if your model supports 250 contexts, and the default contexts is 2, then you should request 248 contexts maximum.
mobile-sp	(Firepower 9300/4100 only) Requests the Mobile SP (GTP/GPRS) license. This license was deprecated in favor of the Carrier license in Version 9.5(2).
strong-encryption	(Chassis only) Requests the Strong Encryption (3DES) license. With FXOS 1.1.3 and later, the Strong Encryption license is automatically enabled for qualified customers when you register the device. Only pre 2.3.0 Smart Software Manager satellite users need to use this command.
tier standard	The standard or essentials tier is the only option available. The Essentials license was formerly called the Standard license.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
License smart configuration	• Yes	• Yes	• Yes	—	• Yes

Command History

Release	Modification
9.3(2)	This command was added.

Release	Modification
9.4(1.152)	Support for the Firepower 9300 ASA security modules, and the **strong-encryption**, **mobile-sp**, and **context** keywords was added.
9.5(2)	The **mobile-sp** keyword was replaced by the **carrier** keyword. The **strong-encryption** keyword was deprecated except for pre 2.3.0 Smart Software Manager satellite users.
9.6(1)	Support for the Firepower 4100 series was added.
9.8(2)	Support for the Firepower 2100 series was added.
9.18(1)	Support for the Secure Firewall 3100 was added, including for the carrier license.

Usage Guidelines

For the ASA Virtual, when you request the feature tier for the first time, you must exit license smart configuration mode for your changes to take effect. If you change the feature tier after you are authorized with the Cisco License Authority, you must reload the ASA Virtual for your changes to take effect.

Examples

The following example sets the ASA Virtual feature tier to standard, and the throughput level to 2G:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

The following example requests 3 contexts on top of the default 2, for a total of 5:

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# feature context 3
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Related Commands

Command	Description
call-home	Configures Smart Call Home. Smart licensing uses Smart Call Home infrastructure.
clear configure license	Clears the smart licensing configuration.
feature tier	Sets the feature tier for smart licensing.
http-proxy	Sets the HTTP(S) proxy for smart licensing and Smart Call Home.
license smart	Lets you request license entitlements for smart licensing.
license smart deregister	Deregisters a device from the License Authority.
license smart register	Registers a device with the License Authority.
license smart renew	Renews the registration or the license entitlement.

Command	Description
service call-home	Enables Smart Call Home.
show license	Shows the smart licensing status.
show running-config license	Shows the smart licensing configuration.
throughput level	Sets the throughput level for smart licensing.

fec

To set Forward Error Correction (FEC) for 25 Gbps and higher interfaces, use the **fec** command in interface configuration mode. To restore the FEC setting to the default, use the **no** form of this command.

Note This command is only supported on the Secure Firewall 3100.

fec { **auto** | **cl108-rs** | **cl74-fc** | **disable** }
no fec { **auto** | **cl108-rs** | **cl74-fc** | **cl91-rs** | **disable** }

Syntax Description

auto	Auto-detects the FEC setting based on the SFP type.
cl108-rs	Sets the FEC mode to Clause 108 RS-FEC.
cl74-fc	Sets the FEC mode to Clause 74 FC-FEC.
cl91-rs	Sets the FEC mode to Clause 91 RS-FEC
disable	Disables FEC.

Command Default

The default setting is **auto**.

Command Modes

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

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

Command History

Release	Modification
9.17(1)	This command was introduced for the Secure Firewall 3100.
9.18(3)/9.19(1)	Default Forward Error Correction (FEC) on Secure Firewall 3100 fixed ports changed to cl108-rs from cl74-fc for 25 GB+ SR, CSR, and LR transceivers.
9.20(1)	Added support for cl91-rs for 100 GB interfaces.

Usage Guidelines

Set the FEC on the physical interface only. You need to set the FEC to EtherChannel member interfaces before you add them to the EtherChannel.

The setting chosen when you use **auto** depends on the transceiver type and whether the interface is fixed (built-in) or on a network module.

Table 1: Default FEC for Auto Setting

Transceiver Type	Fixed Port Default FEC	Network Module Default FEC
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	Auto-Negotiate	Auto-Negotiate
25G-CU4/5M	Auto-Negotiate	Auto-Negotiate
25/50/100G	cl91-rs	cl91-rs

Examples

The following example sets the FEC to cl74-fc:

```
ciscoasa(config)# interface ethernet1/5
ciscoasa(config-if)# fec cl74-fc
```

Related Commands

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

file-bookmarks

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

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

Syntax Description

link	Specifies a change to the links.
title	Specifies a change to the title.
style	Specifies a change to the HTML style.
text	Specifies a change to the text.
value	The actual text or CSS parameters to display (the maximum number is 256 characters).

Command Default

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:

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

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

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

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

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



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

Examples

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

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

Related Commands

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

file-browsing

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

file-browsing enable | disable

Syntax Description

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

Command Default

No default value or behaviors.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The following usage notes apply to file browsing:

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

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

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

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

When you enable or disable an attribute for a DAP record, the ASA applies that value and enforces it. For example, when you disable file browsing in dap webvpn configuration mode, the ASA looks no further for a

value. When you instead set no value for the **file-browsing** command, the attribute is not present in the DAP record, so the ASA moves down to the AAA attribute in the username, and if necessary, the group policy to find a value to apply.

Examples

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

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

Related Commands

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

file-encoding

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

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

Syntax Description

charset	String consisting of up to 40 characters, and equal to one of the valid character sets identified in http://www.iana.org/assignments/character-sets . You can use either the name or the alias of a character set listed on that page. Examples include iso-8859-1, shift_jis, and ibm850. The string is case-insensitive. The command interpreter converts upper case to lower case in the ASA 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 ASA retains the case that you specify, although it ignores the case when matching the name to a server.

Command Default

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:

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

Command History

Release	Modification
7.1(1)	This command was added.

Usage Guidelines

Enter file encoding entries for all CIFS servers that require character encoding entries 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 correct 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 correct 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 of 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:

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

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# file-encoding 10.86.5.174 cp860
ciscoasa(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 webvpn	Displays the running configuration for WebVPN. Use the **all** keyword to include the default configuration.
debug webvpn cifs	Displays debugging messages about the Common Internet File System.

file-entry

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

file-entry enable | **disable**

Syntax Description

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

Command Default

No default value or behaviors.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Dap webvpn configuration	• Yes	• Yes	• Yes	—	—

Command History

Release	Modification
8.0(2)	This command was added.

Usage Guidelines

The ASA can apply attribute values from a variety of sources according to the following hierarchy:

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

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

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

Examples

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

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

Related Commands

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

filter

To specify the name of the access list to use for WebVPN connections for this group policy or username, use the **filter** command in webvpn configuration mode. To remove the access list, use the **no** form of this command.

filter { **value** *ACLname* | **none** }
no filter

Syntax Description

none	Indicates that there is no WebVPN type 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.

Command Default

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:

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

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

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

Examples

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

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(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 configuration mode to configure parameters that apply to group policies or usernames.

filter activex

To remove ActiveX objects in HTTP traffic passing through the ASA, 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* **mask** *foreign_ip foreign_mask*
no filter activex *port* [*-port*] | **except** *local_ip* **mask** *foreign_ip foreign_mask*

Syntax Description

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 the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_ip	The IP address of the highest security level interface from which access is requested. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
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.
-port	(Optional) Specifies a port range.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 that 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 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 ASA cannot block the tag.

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

Examples

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

```
ciscoasa(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 ASA.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies anN2H2 or Websense server for use with the filter command.

filter ftp

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

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

If the Websense or N2H2 server denies the connection, the ASA alters the FTP return code to show that the connection was denied. For example, the ASA 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:

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

Related Commands

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

filter https

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

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

Syntax Description

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

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

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

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

Because HTTPS content is encrypted, the ASA 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:

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter https 443 0 0 0 0
ciscoasa(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 ASA.
filter java	Removes Java applets from HTTP traffic passing through the ASA.
filter url	Directs traffic to a URL filtering server.
show running-config filter	Displays filtering configuration.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

filter java

To remove Java applets from HTTP traffic passing through the ASA, 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

except	(Optional) Creates an exception to a previous filter condition.
foreign_ip	The IP address of the lowest security level interface to which access is requested. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
foreign_mask	Network mask of the foreign_ip argument. Always specify a specific mask value. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_ip	The IP address of the highest security level interface from which access is requested. You can set this address to 0.0.0.0 (or in shortened form, 0) to specify all hosts.
local_mask	Network mask of the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
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.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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

If the <applet> or </applet> HTML tags split across network packets or if the code in the tags is longer than the number of bytes in the MTU, the ASA 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:

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

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

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

Related Commands

filter activex	Removes ActiveX objects from HTTP traffic passing through the ASA.
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 ASA without filtering. If you omit this option, and if the N2H2 or Websense server goes off line, the ASA stops outbound port 80 (Web) traffic until the N2H2 or Websense server is back online.
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 the foreign_ip argument. 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 the *local_ip* argument. You can use 0.0.0.0 (or in shortened form, 0) to specify all hosts.
longurl-deny	Denies the URL request if the URL is over the URL buffer size limit or the URL buffer is not available.
longurl-truncate	Sends only the originating hostname or IP address to the N2H2 or Websense server if the URL is over the URL buffer limit.
-*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 ASA.

Command Default

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 of the filter **url** command determines how the ASA 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 ASA without filtering. If used without the allow option and with the server offline, the ASA stops outbound port 80 (Web) traffic until the server is back online, or if another URL server is available, passes control to the next URL server.

Note With the allow option set, the ASA passes control to an alternate server if the N2H2 or Websense server goes offline.

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

Using the Filtering Server

Websense protocol Version 4 enables group and username authentication between a host and an ASA. The ASA 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 ASA to check outgoing URL requests with the policy defined on the Websense server.
- Username logging tracks username, group, and domain name on the Websense server.

- Username lookup enables the ASA 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:

1. Designate an N2H2 or Websense server with the appropriate vendor-specific form of the url-server command.
2. Enable filtering with the filter command.
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.
4. Use the show url-cache statistics and the show perfmon commands to view run information.

Working with Long URLs

Filtering URLs up to 4 KB is supported for the Websense filtering server, and up to 3 KB for the N2H2 filtering server.

Use the **longurl-truncate** and **cgi-truncate** options to allow handling of URL requests longer than the maximum permitted size.

If a URL is longer than the maximum, and you do not enable the longurl-truncate or longurl-deny options, the ASA drops the packet.

The longurl-truncate option causes the ASA 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 ASA performance.

Buffering HTTP Responses

By default, when a user issues a request to connect to a specific website, the ASA 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:

```
ciscoasa(config)# url-block block
 block-buffer-limit
```

Replace the *block-buffer-limit* argument with the maximum number of blocks that will be buffered. The permitted values are from 1 to 128, which specifies the number of 1550-byte blocks that can be buffered at one time.

Examples

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

```
ciscoasa(config)# url-server (perimeter) host 10.0.1.1
ciscoasa(config)# filter url 80 0 0 0 0
ciscoasa(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:

```
ciscoasa(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 ASA.
filter java	Removes Java applets from HTTP traffic passing through the ASA.
url-block	Manages the URL buffers used for web server responses while waiting for a filtering decision from the filtering server.
url-cache	Enables URL caching while pending responses from an N2H2 or Websense server and sets the size of the cache.
url-server	Identifies an N2H2 or Websense server for use with the filter command.

fips enable

To enable policy checking to enforce FIPS compliance on the system or module, use the fips enable command in global configuration mode. To disable policy checking, use the no form of this command.

fips enable
no fips enable

Syntax Description

enable	Enables or disables policy checking to enforce FIPS compliance.

Command Default

This command has no default settings.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Global configuration	• Yes	• No	• Yes	• Yes	—

Command History

Release	Modification
7.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.
9.8(2)	Enabling FIPS mode now requires you to save your configuration and reload. Also, both units in a failover pair require the same FIPS setting.

Usage Guidelines

To run in a FIPS-compliant mode of operation, you must apply both the fips enable command and the correct configuration specified in the security policy. The internal API allows the device to migrate toward enforcing correct configuration at run time.

When the FIPS-compliant mode 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>
```

Note FIPS mode is not supported in clustering mode.

Note If all interfaces are configured as members of port-channels, then the FIPS self-test will fail during boot. At least one interface must be enabled and not be configured as a member of a port-channel for the FIPS self-test to succeed during boot.

Examples

The following shows policy checking to enforce FIPS compliance on the system:

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot the
 device
```

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 ASA.
show fips	Displays the FIPS current operational state on the ASA.

fips self-test poweron

To execute power-on self-tests, use the fips self-test powereon command in privileged EXEC mode.

fips self-test poweron

Syntax Description

poweron	Executes power-on self-tests.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was added.
9.0(1)	Support for multiple context mode was added.

Usage Guidelines

Entering this command causes the device to run all self-tests required for FIPS 140-2 compliance. Tests include the cryptographic algorithm test, software integrity test, and critical functions test.

Examples

The following example shows the system executing power-on of self-tests:

```
ciscoasa(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 disables 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 ASA.

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.

firewall transparent
no firewall transparent

Syntax Description

This command has no arguments or keywords.

Command Default

By default, the ASA is in routed mode.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
8.5(1)/9.0(1)	You can set this per context in multiple context mode.

Usage Guidelines

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.

You can set this command per context in multiple context mode.

When you change modes, the ASA 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 ASA that changes the mode with the **firewall transparent** command, be sure to put the command at the top of the configuration; the ASA 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 ASA clears all the preceding lines in the configuration.

Examples

The following example changes the firewall mode to transparent:

```
ciscoasa(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.

flow-export active refresh-interval

To specify the time interval between flow-update events, use the **flow-export active refresh-interval** command in global configuration mode.

flow-export active refresh-interval *value*

Syntax Description

value	Specifies the time interval between flow-update events in minutes. Valid values are from 1-60 minutes.

Command Default

The default value is 1 minute.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was added.

Usage Guidelines

If you have already configured the **flow-export delay flow-create** command, and you then configure the flow-export active refresh-interval command with an interval value that is not at least 5 seconds more than the delay value, the following warning message appears at the console:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
 appear before flow-creation events.
```

If you have already configured the flow-export active refresh-interval command, and you then configure the **flow-export delay flow-create** command with a delay value that is not at least 5 seconds less than the interval value, the following warning message appears at the console:

```
WARNING: The current delay flow-create value configuration may cause flow-update events to
 appear before flow-creation events.
```

Examples

The following example shows how to configure a time interval of 30 minutes:

```
ciscoasa(config)# flow-export active refresh-interval 30
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.

Commands	Description
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export delay flow-create

To delay export of the flow-create event, use the **flow-export delay flow-create** command in global configuration mode. To export the flow-create event without a delay, use the **no** form of this command.

flow-export delay flow-create *seconds*
no flow-export delay flow-create *seconds*

Syntax Description

seconds	Specifies the delay in seconds for exporting the flow-create event. Valid values are 1-180 seconds.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.1(2)	This command was added.

Usage Guidelines

If the flow-export delay flow-create command is not configured, the flow-create event is exported without a delay.

If the flow is torn down before the configured delay, the flow-create event is not sent; an extended flow teardown event is sent instead.

Examples

The following example shows how to delay the export of a flow-create event by ten seconds:

```
ciscoasa(config)# flow-export delay flow-create 10
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.

Commands	Description
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export destination

To configure a collector to which NetFlow packets are sent, use the **flow-export destination** command in global configuration mode. To remove a collector of NetFlow packets, use the **no** form of this command.

flow-export destination *interface-name ipv4-address | hostname udp-port*
no flow-export destination *interface-name ipv4-address | hostname udp-port*

Syntax Description

hostname	Specifies the hostname of the NetFlow collector.
interface-name	Specifies the name of the interface through which the destination can be reached.
ipv4-address	Specifies the IP address of the NetFlow collector. Only IPv4 is supported.
udp-port	Specifies the UDP port on which the NetFlow collector is listening. Valid values are 1-65535.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	This command was added.
8.1(2)	The maximum number of flow export destinations was increased to five.

Usage Guidelines

You can use the flow-export destination command to configure the ASA to export NetFlow data to a NetFlow collector.

Note You can enter a maximum of five export destinations (collectors) per security context. When you enter a new destination, the template records are sent to the newly added collector. If you try to add more than five destinations, the following error message appears:“ERROR: A maximum of 5 flow-export destinations can be configured.”

If the ASA is configured to export NetFlow data, to improve performance, we recommend that you disable redundant syslog messages (those also captured by NetFlow) by entering the **logging flow-export-syslogs disable** command.

Examples

The following example shows how to configure a collector for NetFlow data:

```
ciscoasa(config)# flow-export destination inside 209.165.200.224 2055
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.
low-export delay flow-create	Delays the export of the flow-create event by a specified amount of time.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export event-type destination

To configure the address of NetFlow collectors and filters to determine which NetFlow records should be sent to each collector, use the **flow-export event-type destination** command in policy-map class configuration mode. To remove the address of NetFlow collectors and filters, use the **no** form of this command.

flow-export event-type { **all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown** } **destination**
no flow-export event-type { **all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown** } **destination**

Syntax Description

all	Specifies all four event types.
flow-create	Specifies flow-create events.
flow-denied	Specifies flow-denied events.
flow-teardown	Specifies flow-teardown events.
flow-update	Specifies flow-update events.

Command Default

No default behavior or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Policy-map class configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.1(2)	This command was added.

Usage Guidelines

NetFlow events are configured through Modular Policy Framework. If Modular Policy Framework is not configured for NetFlow, no events are logged. Traffic is matched based on the order in which classes are configured. After a match is detected, no other classes are checked. For NetFlow events, the configuration requirements are as follows:

- A flow-export destination (that is, a NetFlow collector) is uniquely identified by its IP address.
- Supported event types are flow-create, flow-teardown, flow-denied, flow-update, and all, which include the four previously listed event types.
- Flow-export actions are not supported in interface policies.
- Flow-export actions are only supported in the **class-default** command and in classes with the **match any** or **match access-list** command.

- If no NetFlow collector has been defined, no configuration actions occur.
- NetFlow Secure Event Logging filtering is order-independent.

Note To create a valid NetFlow configuration, you must have both the flow-export destination configuration and the flow-export event-type configuration. The flow-export destination configuration alone does nothing. You must also configure a class map for the flow-export event-type configuration. This can either be the default class map or one that you create.

Examples

The following example exports all NetFlow events between hosts 10.1.1.1 and 20.1.1.1 to the destination 15.1.1.1.

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

Related Commands

Commands	Description
clear flow-export counters	Resets all runtime counters in NetFlow to zero.
flow-export delay flow-create	Delays the export of the flow-create event by a specified amount of time.
flow-export template timeout-rate	Controls the interval at which the template information is sent to the NetFlow collector.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-export template timeout-rate

To control the interval at which the template information is sent to NetFlow collectors, use the **flow-export template timeout-rate** command in global configuration mode. To reset the template timeout to the default value, use the **no** form of this command.

flow-export template timeout-rate *minutes*
no flow-export template timeout-rate *minutes*

Syntax Description

minutes	Specifies the interval in minutes. Valid values are 1-3600 minutes.
template	Enables the **timeout-rate** keyword for configuring export templates.
timeout-rate	Specifies the amount of time elapsed (interval) after the template is initially sent before it is resent.

Command Default

The default value for the interval is 30 minutes.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	This command was added.

Usage Guidelines

You should configure the timeout rate based on the collector being used and at what rate the collectors expect the templates to be refreshed.

If the security appliance is configured to export NetFlow data, to improve performance, we recommend that you disable redundant syslog messages (those also captured by NetFlow) by entering the **logging flow-export-syslogs disable** command.

Examples

The following example shows how to configure NetFlow to send template records to all collectors every 60 minutes:

```
ciscoasa(config)# flow-export template timeout-rate 60
```

Related Commands

Commands	Description
clear flow-export counters	Resets all the runtime counters associated with NetFlow data.
flow-export destination	Specifies the IP address or hostname of the NetFlow collector, and the UDP port on which the NetFlow collector is listening.
logging flow-export-syslogs enable	Enables syslog messages after you have entered the **logging flow-export-syslogs disable** command, and the syslog messages that are associated with NetFlow data.
show flow-export counters	Displays a set of runtime counters for NetFlow.

flow-offload cluster-redirect

To enable cluster redirect on the Secure Firewall 4200, use the **flow-offload cluster-redirect** command in global configuration mode. To disable cluster redirect, use the **no** form of this command.

flow-offload cluster-redirect
no flow-offload cluster-redirect

Syntax Description

This command has no arguments or keywords.

Command Default

Cluster redirect is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.23(1)	This command was introduced for the Secure Firewall 4200.

Usage Guidelines

For asymmetric flows, cluster redirect lets the forwarding node offload flows to hardware. When traffic for an existing flow is sent to a different node, then that traffic is redirected to the owner node over the cluster control link. Because asymmetric flows can create a lot of traffic on the cluster control link, letting the forwarder offload these flows can improve performance.

The **flow-offload enable** command must be enabled for this command to work. **flow-offload enable** is also enabled by default.

Examples

The following example disables cluster redirect.

```
ciscoasa(config)# no flow-offload cluster-redirect
```

Related Commands

Command	Description
flow-offload enable	Enables flow offload.
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.
show flow-offload	Displays information about flow off-loading.

flow-offload enable

To enable flow off-loading, use the **flow-offload enable** command in global configuration mode. To disable the off-loading, use the **no** form of this command.

flow-offloadenable
no flow-offload enable

Syntax Description

This command has no arguments or keywords.

Command Default

Flow off-loading is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.5(2.1)	This command was introduced. It is available for the Firepower 9300 series running FXOS 1.1.3+ only.
9.6(1)	Support was added for the Firepower 4100 series running FXOS 1.1.4+.
9.6(2)	Support was added for multicast connections in transparent mode, but only for bridge groups that contain two and only two interfaces.
9.15(1)	A reload is only required at initial enabling for the Firepower 4100/9300.
9.17(1)	Support was added for the Secure Firewall 3100.
9.20(1)	Support was added for the Secure Firewall 4200.
9.23(1)	Flow offload is enabled by default for the Secure Firewall 3100/4200.

Usage Guidelines

If you deploy a appliance with an ASA security module in a data center, you can identify select traffic to be off-loaded to a super fast path, where the flows are switched in the NIC itself. Off-loading can help you improve performance for data-intensive applications such as large file transfers.

Before being off-loaded, the ASA first applies normal security processing, such as access rules and inspection, during connection establishment. The ASA also does session tear-down. But once a connection is established, if it is eligible to be off-loaded, further processing happens in the NIC rather than the ASA.

While offloaded, the flow does not receive security policy checking or other services, so that it can move through the system as fast as possible. For off-loaded flows, there is no inspection, TCP normalization (except for checksum verification, if you configure it), QoS, or sequence number checking.

To identify flows that can be off-loaded, you create a service policy rule that applies the flow off-loading service. A matching flow is then off-loaded if it meets the following conditions:

- IPv4 addresses only.
- TCP, UDP, GRE only.
- Standard or 802.1q tagged Ethernet frames only.
- (Transparent mode only.) Multicast flows for bridge groups that contain two and only two interfaces.
- It is not receiving services that cannot be applied to off-loaded flows, such as inspection, decryption, IPSec and VPN flows, or flows directed to a service module.

Reverse flows for off-loaded flows are also off-loaded.

In multiple-context mode, enabling or disabling flow offload enables or disables it for all contexts. You cannot have different settings per context.

Prior to 9.15(1) on the Firepower 4100/9300, you must reload the system whenever you enable or disable flow offload. Starting with version 9.15(1), a reload is only required the first time you enable flow offload. Reloading is not required for the Secure Firewall 3100/4200. When a reload is required, there are special considerations for changing the mode for clusters or failover pairs if you want a hitless change:

- Clustering—First enter the command on the control node, but do not reboot the control node immediately. Instead, reboot each node of the cluster first, then return to the control node and reboot it. You can then configure the offloading service policy on the control node.
- Failover—First enter the command on the active unit, but do not reboot it immediately. Instead, reboot the standby unit, then reboot the active unit. You can then configure the offloading service policy on the active unit.



Note For more specific information on device support, see http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/compatibility/fxos-compatibility.html .

Examples

The following example enables flow off-loading, saves the configuration, and reboots the system.

```
ciscoasa(config)# flow-offload enable

WARNING: This command will take effect after the running-config is
saved and the system has been rebooted.
ciscoasa(config)# write memory

ciscoasa(config)# reload
```

Related Commands

Command	Description
set-connection advanced-options flow-offload	Identifies traffic flows as eligible for off-load.

Command	Description
show flow-offload	Displays information about flow off-loading.

flow-offload-dtls

To enable DTLS crypto acceleration on the device, use the **flow-offload-dtls** command in global configuration mode. To disable this feature, use the **no** form of this command.

flow-offload-dtls

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.22(1)	The command was introduced.

Usage Guidelines

The Cisco Secure Firewall 4200 and 3100 series devices, with the help of the FPGA and the Nitrox V crypto accelerator, support DTLS cryptographic acceleration. This feature improves the throughput of the DTLS encrypted and decrypted traffic. Both IPv4 and IPv6 traffic is supported. This feature works only for DTLS 1.2.

Supported Devices

- Cisco Secure Firewall 4200 Series: 4215, 4225, 4245
- Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140

Supported Network Processing Unit FPGA Firmware Versions

- Cisco Secure Firewall 4200 Series: 1024.11.00
- Cisco Secure Firewall 3100 Series:
  - 3100 Low SKU: 1792.4.00
  - 3100 High SKU: 1792.3.00

If you upgrade your devices to Version 9.22(1) and later, the firmware is automatically upgraded.

To view the Network Processing Unit (NPU) FPGA firmware of the device, use the **show version detail | inc Fpga** command:

```
device# show version detail | inc Fpga
Fpga-Vers: 0.21.00
Fpga-Golden-Vers: 0.21.00
```

```
NpuFpga-Vers: 1792.4.00
TamFpga-Vers: 2.6.d
Epm-Fpga-Version: UNKNOWN
```

Example

The following example enables DTLS crypto acceleration on the device.

```
ciscoasa# flow-offload-dtls
```

Related Commands

Command	Description
flow-offload-dtls egress-optimization	Enables optimization of egress encrypted packets and improve latency.
show flow-offload-dtls info	Displays IPsec flow offload information.
show flow-offload-dtls statistics	Displays IPsec flow offload statistics.

flow-offload-dtls

To enable DTLS crypto acceleration on the device, use the **flow-offload-dtls** command in global configuration mode. To disable this feature, use the **no** form of this command.

flow-offload-dtls

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.22(1)	The command was introduced.

Usage Guidelines

The Cisco Secure Firewall 4200 and 3100 series devices, with the help of the FPGA and the Nitrox V crypto accelerator, support DTLS cryptographic acceleration. This feature improves the throughput of the DTLS encrypted and decrypted traffic. Both IPv4 and IPv6 traffic is supported. This feature works only for DTLS 1.2.

Supported Devices

- Cisco Secure Firewall 4200 Series: 4215, 4225, 4245
- Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140

Supported Network Processing Unit FPGA Firmware Versions

- Cisco Secure Firewall 4200 Series: 1024.11.00
- Cisco Secure Firewall 3100 Series:
  - 3100 Low SKU: 1792.4.00
  - 3100 High SKU: 1792.3.00

If you upgrade your devices to Version 9.22(1) and later, the firmware is automatically upgraded.

To view the Network Processing Unit (NPU) FPGA firmware of the device, use the **show version detail | inc Fpga** command:

```
device# show version detail | inc Fpga
Fpga-Vers: 0.21.00
Fpga-Golden-Vers: 0.21.00
```

```
NpuFpga-Vers: 1792.4.00
TamFpga-Vers: 2.6.d
Epm-Fpga-Version: UNKNOWN
```

Example

The following example enables DTLS crypto acceleration on the device.

```
ciscoasa# flow-offload-dtls
```

Related Commands

Command	Description
flow-offload-dtls egress-optimization	Enables optimization of egress encrypted packets and improve latency.
show flow-offload-dtls info	Displays IPsec flow offload information.
show flow-offload-dtls statistics	Displays IPsec flow offload statistics.

flow-offload-dtls egress-optimization

To enable optimization of egress encrypted packets and improve latency, use the **flow-offload-dtls egress-optimization** command in global configuration mode. To disable this feature, use the **no** form of this command.

flow-offload-dtls egress-optimization

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
9.22(1)	The command was introduced.

Usage Guidelines

This feature works only for DTLS 1.2. The hardware performs optimization of the egress encrypted packets to improve latency. The data path is optimized to enhance performance for single tunnel flows. Both IPv4 and IPv6 traffic is supported.

Supported Devices

- Cisco Secure Firewall 4200 Series: 4215, 4225, 4245
- Cisco Secure Firewall 3100 Series: 3105, 3110, 3120, 3130, 3140

Supported Network Processing Unit FPGA Firmware Versions

- Cisco Secure Firewall 4200 Series: 1024.11.00
- Cisco Secure Firewall 3100 Series:
  - 3100 Low SKU: 1792.4.00
  - 3100 High SKU: 1792.3.00

If you upgrade your devices to Version 9.22(1) and later, the firmware is automatically upgraded.

To view the Network Processing Unit (NPU) FPGA firmware of the device, use the **show version detail | inc Fpga** command:

```
device# show version detail | inc Fpga
Fpga-Vers: 0.21.00
Fpga-Golden-Vers: 0.21.00
```

```
NpuFpga-Vers: 1792.4.00
TamFpga-Vers: 2.6.d
Epm-Fpga-Version: UNKNOWN
```

Example

The following example enables optimization of egress encrypted packets and improves latency.

```
ciscoasa# flow-offload-dtls egress-optimization
```

Related Commands

Command	Description
flow-offload-dtls	Enables DTLS crypto acceleration on the device.
show flow-offload-dtls info	Displays IPsec flow offload information.
show flow-offload-dtls statistics	Displays IPsec flow offload statistics.

flow-offload-ipsec

To enable IPsec flow off-loading, use the **flow-offload-ipsec** command in global configuration mode. To disable the off-loading, use the **no** form of this command.

flow-offload-ipsec [**egress-optimization**]
no flow-offload-ipsec [**egress-optimization**]

Syntax Description

egress-optimization	(Optional.) Optimize the data path to enhance performance for single tunnel flows.

Command Default

IPsec flow offload is enabled on default platforms that support it, but egress optimization is disabled by default.

Command Modes

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

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

Command History

Release	Modification
9.18(1)	The command was introduced for the Secure Firewall 3100.
9.20(1)	Support was added for the Secure Firewall 4200.
9.22(1)	Support was added for the Secure Firewall 1200.
9.23(1)	Support was added for IPsec flow offload for traffic on the cluster control link on the Secure Firewall 4200 in distributed site-to-site VPN mode.

Usage Guidelines

You can configure supporting device models to use IPsec flow offload. After the initial setup of an IPsec site-to-site VPN or remote access VPN security association (SA), IPsec connections are offloaded to the field-programmable gate array (FPGA) in the device, which should improve device performance. On the Secure Firewall 1200 series, IPsec connections are offloaded to the Marvell Cryptographic Accelerator (CPT) to improve device performance.On the Secure Firewall 6100 series, IPsec connections are offloaded to the Kintex 7 (KC400) FPGA. This FPGA contains a built-in crypto engine that is capable of handling AES-GCM-128 and AES-GCM-256 encryption and decryption.

Offloaded operations specifically relate to the pre-decryption and decryption processing on ingress, and the pre-encryption and encryption processing on egress. The system software handles the inner flow to apply your security policies.

IPsec flow offload is enabled by default, and applies to the following device types:

- Secure Firewall 1200

- Secure Firewall 3100
- Secure Firewall 4200
- Secure Firewall 6100

IPsec flow offload is also used when the device's VTI loopback interface is enabled.

For asymmetric flows in cluster distributed site-to-site VPN mode, IPsec flow offload now lets the flow owner decrypt IPsec traffic in hardware that was forwarded over the cluster control link. This feature is not configurable and is always available with IPsec flow offload.

The following IPsec flows are not offloaded:

- KEv1 tunnels. Only IKEv2 tunnels will be offloaded. IKEv2 supports stronger ciphers.
- Flows that have volume-based rekeying configured.
- Flows that have compression configured.
- Transport mode flows. Only tunnel mode flows will be offloaded.
- AH format. Only ESP/NAT-T format will be supported.
- Flows that have post-fragmentation configured.
- Flows that have anti-replay window size other than 64bit and anti-replay is not disabled.
- Flows that have firewall filter enabled.
- Multiple context mode.
- Secure Firewall 6100 supports AES-GCM-128 and AES-GCM-256 ciphers only. IPsec tunnels that are configured with other ciphers are not offloaded. Any IPsec packets that are not offloaded are processed by the software engine in the CPU.

Example

The following example enables both IPsec flow offload and egress optimization.

```
ciscoasa# flow-offload-ipsec
ciscoasa# flow-offload-ipsec egress-optimization
```

Related Commands

Command	Description
clear flow-offload-ipsec	Clears IPsec flow offload statistics.
show flow-offload-ipsec	Displays IPsec flow offload statistics and information.

flowcontrol

To enable pause (XOFF) frames for flow control, use the **flowcontrol** command in interface configuration mode. To disable pause frames, use the **no** form of this command.

Secure Firewall 3100:

flowcontrol send on
no flowcontrol send on

ASA Hardware:

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]
no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

Syntax Description

high_water	Sets the high-water mark between 0 and 511 KB for 10 GigabitEthernet, and between 0 and 47 KB for 1 GigabitEthernet (or 0 and 11 KB for GigabitEthernet interfaces on the 4GE-SSM). When the buffer usage exceeds the high-water mark, the NIC sends a pause frame.
low_water	Sets the low-water mark between 0 and 511 KB for 10 GigabitEthernet, and between 0 and 47 KB for 1 GigabitEthernet (or 0 and 11 KB for GigabitEthernet interfaces on the 4GE-SSM). After the network interface controller (NIC) sends a pause frame, when the buffer usage is reduced below the low-water mark, the NIC sends an XON frame. The link partner can resume traffic after receiving an XON frame.
noconfirm	Applies the command without confirmation. Because this command resets the interface, without this option, you are asked to confirm the configuration change.
pause_time	Sets the pause refresh threshold value, between 0 and 65535 slots. Each slot is the amount of time to transmit 64 bytes, so the time per unit depends on your link speed. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by this timer value in the pause frame. If the buffer usage is consistently above the high watermark, pause frames are sent repeatedly, controlled by the pause refresh threshold value. The default is 26624.

Command Default

Pause frames are disabled by default.

For the Secure Firewall 3100, see the following values (not configurable):

- The global high watermark is 2 MB (8000 buffers).
- The global low watermark is 1.25 MB (5000 buffers).
- The port high watermark is .3125 MB (1250 buffers).
- The port low watermark is .25 MB (1000 buffers).

For ASA hardware 10 GigabitEthernet, see the following default settings:

- The default high watermark is 128 KB.
- The default low watermark is 64 KB.
- The default pause refresh threshold value is 26624 slots.

For For ASA hardware 1 GigabitEthernet, see the following default settings:

- The default high watermark is 24 KB.
- The default low watermark is 16 KB.
- The default pause refresh threshold value is 26624 slots.

Command Modes

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

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

Command History

Release	Modification
8.2(2)	This command was added for 10-GigabitEthernet interfaces on the ASA 5580.
8.2(3)	Added support for the ASA 5585-X.
8.2(5)/8.4(2)	Added support for 1-GigabitEthernet interfaces on all models.
9.18(1)	Added support for the Secure Firewall 3100.

Usage Guidelines

This command is supported on 1-GigabitEthernet and higher interfaces. This command does not support management interfaces.

Enter this command for a physical interface.

Note Only flow control frames defined in 802.3x are supported. Priority-based flow control is not supported.

Secure Firewall 3100

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If the ASA port experiences congestion (exhaustion of queuing resources on the internal switch) and cannot receive any more traffic, it notifies the other port by sending a pause frame to stop sending until the condition clears. Upon receipt of a pause frame, the sending device stops sending any data packets, which prevents any loss of data packets during the congestion period.

Note The ASA supports transmitting pause frames so that the remote peer can rate-control the traffic.

However, receiving of pause frames is not supported.

The internal switch has a global pool of 8000 buffers of 250 bytes each, and the switch allocates buffers dynamically to each port. A pause frame is sent out every interface with flowcontrol enabled when the buffer usage exceeds the global high-water mark (2 MB (8000 buffers)); and a pause frame is sent out of a particular interface when its buffer exceeds the port high-water mark (.3125 MB (1250 buffers)). After a pause is sent, an XON frame can be sent when the buffer usage is reduced below the low-water mark (1.25 MB globally (5000 buffers); .25 MB per port (1000 buffers)). The link partner can resume traffic after receiving an XON frame.

ASA Hardware

If you have a traffic burst, dropped packets can occur if the burst exceeds the buffering capacity of the FIFO buffer on the NIC and the receive ring buffers. Enabling pause frames for flow control can alleviate this issue.

When you enable this command, pause (XOFF) and XON frames are generated automatically by the NIC hardware based on the FIFO buffer usage:

1. The NIC sends a pause frame when the buffer usage exceeds the high watermark.
2. After a pause is sent, the NIC sends an XON frame when the buffer usage is reduced below the low watermark.
3. The link partner can resume traffic after receiving an XON, or after the XOFF expires, as controlled by the timer value in the pause frame.
4. If the buffer usage is consistently above the high watermark, the NIC sends pause frames repeatedly, controlled by the pause refresh threshold value.

When you use this command on ASA models, the following warning message appears:

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

To change the parameters without being prompted, use the **noconfirm** keyword.

Examples

The following example enables pause frames using the default settings:

```
ciscoasa(config)# interface tengigabitethernet 1/0
ciscoasa(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
ciscoasa(config-if)# y
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

flow-mobility lisp

To enable flow mobility for the cluster, use the **flow-mobility lisp** command in cluster configuration mode. To disable flow mobility, use the **no** form of this command.

flow-mobility lisp
no flow-mobility lisp

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
9.5(2)	This command was added.

Usage Guidelines

This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications.

About LISP Inspection for Cluster Flow Mobility

The ASA inspects LISP traffic for location changes and then uses this information for seamless clustering operation. With LISP integration, the ASA cluster members can inspect LISP traffic passing between the first hop router and the ETR or ITR, and can then change the flow owner to be at the new site.

Cluster flow mobility includes several inter-related configurations:

1. (Optional) Limit inspected EIDs based on the host or server IP address—The first hop router might send EID-notify messages for hosts or networks the ASA cluster is not involved with, so you can limit the EIDs to only those servers or networks relevant to your cluster. For example, if the cluster is only involved with 2 sites, but LISP is running on 3 sites, you should only include EIDs for the 2 sites involved with the cluster. See the **policy-map type inspect lisp**, **allowed-eid,** and **validate-key** commands.
2. LISP traffic inspection—The ASA inspects LISP traffic for the EID-notify message sent between the first hop router and the ITR or ETR. The ASA maintains an EID table that correlates the EID and the site ID. For example, you should inspect LISP traffic with a source IP address of the first hop router and a destination address of the ITR or ETR. See the **inspect lisp** command.
3. Service Policy to enable flow mobility on specified traffic—You should enable flow mobility on business-critical traffic. For example, you can limit flow mobility to only HTTPS traffic, and/or to traffic to specific servers. See the **cluster flow-mobility lisp** command.

4. Site IDs—The ASA uses the site ID for each cluster unit to determine the new owner. See the **site-id** command.
5. Cluster-level configuration to enable flow mobility—You must also enable flow mobility at the cluster level. This on/off toggle lets you easily enable or disable flow mobility for a particular class of traffic or applications. See the **flow-mobility lisp** command.

Examples

The following example enables flow mobility for cluster1:

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# flow-mobility lisp
```

Related Commands

Command	Description
allowed-eids	Limits inspected EIDs based on IP address.
clear cluster info flow-mobility counters	Clears the flow mobility counters.
clear lisp eid	Removes EIDs from the ASA EID table.
cluster flow-mobility lisp	Enables flow mobility for the service policy.
flow-mobility lisp	Enables flow mobility for the cluster.
inspect lisp	Inspects LISP traffic.
policy-map type inspect lisp	Customizes the LISP inspection.
site-id	Sets the site ID for a cluster chassis.
show asp table classify domain inspect-lisp	Shows the ASP table for LISP inspection.
show cluster info flow-mobility counters	Shows flow mobility counters.
show conn	Shows traffic subject to LISP flow-mobility.
show lisp eid	Shows the ASA EID table.
show service-policy	Shows the service policy.
validate-key	Enters the preshared key to validate LISP messages.

force re-authentication

To allow an identity provider to authenticate directly rather than rely on a previous security context when a SAML authentication request occurs, use the force re-authentication command in saml idp webvpn configuration mode. To disable this setting, use the no form of this command.

force re-authentication

Command Default

By default, this setting is enabled.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
webvpn	• Yes	• Yes	• Yes	• Yes	—

Usage Guidelines

ASA must have the SAML configuration. This command is necessary when you require direct re-authentication with the IdP.

Example

The following example shows this command:

```
ciscoasa(config-webvpn-saml-idp)# force re-authentication
```

Related Commands

Command	Description
saml idp	Adds a new SAML IdP.

format

To erase all files and format the file system, use the **format** command in privileged EXEC mode.

format { **disk0:** | **disk1:** | **flash:** }

Syntax Description

disk0:	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. In the ASA 5500 series, the **flash** keyword is aliased to **disk0**.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

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 the ASA 5500 series, the **erase** command destroys all user data on the disk with the 0xFF pattern. In contrast, the **format** command only resets the file system control structures. If you used a raw disk read tool, you could still see the information. To repair a corrupt file system, try entering the **fsck** command before entering the **format** command.

Examples

This example shows how to format the flash memory:

```
ciscoasa# format flash:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the flash memory.
fsck	Repairs a corrupt file system.

forward interface

For models with a built-in switch, such as the ASA 5505, use the **forward interface** command in interface configuration mode to restore connectivity for one VLAN from initiating contact to one other VLAN. To restrict one VLAN from initiating contact to one other VLAN, use the **no** form of this command.

forward interface vlan *number*
no forward interface vlan *number*

Note Supported for the Firepower 1010 and ASA 5505 only.

Syntax Description

vlan *number*	Specifies the VLAN ID to which this VLAN interface cannot initiate traffic.

Command Default

By default, all interfaces can initiate traffic to all other interfaces.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was added.
9.13(1)	Support for the Firepower 1010 was added.

Usage Guidelines

You might need to restrict one VLAN depending on how many VLANs your license supports.

In routed mode, you can configure up to three active VLANs with the ASA 5505 Base license, and up to five active VLANs with the Security Plus license. An active VLAN is a VLAN with a **nameif** command configured. You can configure up to five inactive VLANs on the ASA 5505 for either license, but if you make them active, be sure to follow the guidelines for your license.

With the Base license, the third VLAN must be configured with the **no forward interface** command to restrict this VLAN from initiating contact to one other VLAN.

For example, you have one VLAN assigned to the outside for Internet access, one VLAN assigned to an inside work network, and a third VLAN assigned to your home network. The home network does not need to access

the work network, so you can use the **no forward interface** command on the home VLAN; the work network can access the home network, but the home network cannot access the work network.

If you already have two VLAN interfaces configured with a **nameif** command, be sure to enter the **no forward interface** command before the **nameif** command on the third interface; the ASA does not allow three fully functioning VLAN interfaces with the Base license on the ASA 5505.

Examples

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work interface.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
...
```

Related Commands

Command	Description
backup interface	Assigns an interface to be a backup link to an ISP, for example.
clear interface	Clears counters for the **show interface** command.
interface vlan	Creates a VLAN interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
switchport	Sets an interface to switch port mode.
switchport access vlan	Assigns a switch port to a VLAN.

forward-reference (Deprecated)

To make it possible to refer to ACLs and objects that do not yet exist, use the **forward-reference** command in global configuration mode.

forward-reference enable
no forward-reference enable

Syntax Description

enable	Enables forward referencing of ACLs (in access groups) and objects (in objects and ACLs).

Command Default

(Pre-9.18) The default is that forward-referencing is disabled. An ACL or object must exist to be able to refer to it in an access list rule, another object, or an access group.

Starting with 9.18, this command is enabled by default, and you can no longer configure it. Forward referencing is always enabled.

Command Modes

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

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

Command History

Release	Modification
9.3(2)	This command was added.
9.18(1)	This command was removed. The default was changed to enabled at all times. You cannot change this behavior.

Usage Guidelines

This command is most useful when used in conjunction with the **configure session** command, which creates isolated sessions for editing ACLs and their objects. For example, within a session, you could delete an ACL that is currently referenced by an **access-group** command, and create a new ACL with the same name. After committing the session, the new version of the ACL is compiled, and after compilation, becomes the active version of the access group.

Similarly, you can delete and recreate objects that are used by active access rules.

Forward referencing is designed for access rule ACL usage. You cannot delete an object currently used by other features, such as NAT or VPN.

Enable forward referencing with caution. The default behavior ensures that you do not make simple typos when configuring objects, access lists, and access groups. With forward referencing, the ASA cannot tell the difference between a typo and an intentional reference to something you intend to create in the future.

Any rule, access group, or object that points to a non-existent object or ACL is ignored during operation. It does not become operational until you create the missing item.

Examples

The following example enables forward referencing:

```
ciscoasa(config)# forward-reference enable
```

Related Commands

Command	Description
access-group	Assigns an ACL to an interface or globally.
access-list	Creates ACL rules.
configure session	Creates or opens a session.
object	Creates an object.
object-group	Creates an object group.

fqdn (crypto ca trustpoint)

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

fqdn [*fqdn* | **none**]
no fqdn

Syntax Description

fqdn	Specifies the FQDN. The maximum length is 64 characters.
none	Specifies no fully qualified domain name.

Command Default

The default setting does not include the FQDN.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Crypto ca-trustpoint configuration	• Yes	• Yes	• Yes	• Yes	• Yes

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

If you are configuring the ASA to support authentication of a Nokia VPN Client using certificates, use the **none** keyword. See the **crypto isakmp identity** or **isakmp identity** command for more information about supporting certificate authentication of the Nokia VPN Client.

Examples

The following example enters crypto ca-trustpoint configuration mode for the trustpoint central, and includes the FQDN engineering in the enrollment request for the trustpoint central:

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# fqdn engineering
ciscoasa(config-ca-trustpoint)#
```

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

Command	Description
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.
enrollment retry period	Specifies the number of minutes to wait before trying to send an enrollment request.
enrollment terminal	Specifies cut-and-paste enrollment with this trustpoint.

fqdn (network object)

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

fqdn [**v4** | **v6**] *fqdn*
no fqdn [**v4** | **v6**] *fqdn*

Syntax Description

fqdn	Specifies the FQDN, including the host and domain. The FQDN must begin and end with a digit or letter. Only letters, digits, and hyphens are allowed as internal characters. Labels are separated by a dot (for example, www.cisco.com).
v4	(Optional) Specifies an IPv4 domain name.
v6	(Optional) Specifies an IPv6 domain name.

Command Default

By default, the domain name is an IPv4 domain.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
Object network configuration	• Yes	• Yes	• Yes	• Yes	—

Command History

Release	Modification
8.4(2)	This command was added.

Usage Guidelines

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

Examples

The following example shows how to create a network object:

```
ciscoasa (config)# object network FQDN_1
ciscoasa (config-network-object)# fqdn example.cisco.com
```

Related Commands

Command	Description
clear configure object	Clears all objects created.
description	Adds a description to the network object.

Command	Description
fqdn	Specifies a fully qualified domain name network object.
host	Specifies a host network object.
nat	Enables NAT for the network object.
object network	Creates a network object.
object-group network	Creates a network object group.
range	Specifies a range of addresses for the network object.
show running-config object network	Shows the network object configuration.
subnet	Specifies a subnet network object.

fragment

To provide additional management of packet fragmentation and improve compatibility with NFS, use the fragment command in global configuration mode. To return to the default values, use the **no** form of this command.

fragment reassembly { **full** | **virtual** } { **size** | **chain** | **timeout** *limit* } [*interface*]
no fragment reassembly { **full** | **virtual** } { **size** | **chain** | **timeout** *limit* } [*interface*]

Syntax Description

chain limit	Specifies the maximum number of fragments into which a full IP packet can be fragmented.
interface	(Optional) Specifies the ASA interface. If an interface is not specified, the command applies to all interfaces.
reassembly full | **virtual**	Specifies the full or virtual reassembly for IP fragments that are routed through the ASA. IP fragments that terminate at the ASA are always fully reassembled.
size limit	Sets the maximum number of fragments that can be in the IP reassembly database waiting for reassembly. **Note** The ASA 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.

Command Default

The defaults are as follows:

- **chain** is 24 packets.
- *interface* is all interfaces.
- **size** is 200.
- **timeout** is 5 seconds.
- Virtual reassembly is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified so that you now must choose one of the following keywords: **chain**, **size**, or **timeout**. You can no longer enter the **fragment** command without entering one of these keywords, as was supported in prior releases of the software.
8.0(4)	The **reassembly full** | **virtual** option was added.

Usage Guidelines

By default, the ASA accepts up to 24 fragments to reconstruct a full IP packet. Based on your network security policy, you should consider configuring the ASA to prevent fragmented packets from traversing the ASA 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 ASA 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 ASA 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.

The following processes are performed regardless of the **reassembly** option setting:

- IP fragments are collected until a fragment set is formed or until a timeout interval has elapsed (see the **timeout** option).
- If a fragment set is formed, integrity checks are performed on the set. These checks include no overlapping, no tail overflow, and no chain overflow (see the **chain** option).

If the **fragment reassembly virtual** command is configured, the fragment set is forwarded to the transport layer for further processing.

If the **fragment reassembly full** command is configured, the fragment set is first coalesced into a single IP packet. The single IP packet is then forwarded to the transport layer for further processing.

Examples

The following example shows how to prevent fragmented packets on the outside and inside interfaces:

```
ciscoasa(config)# fragment chain 1 outside
ciscoasa(config)# fragment chain 1 inside
```

Continue entering the fragment chain 1 interface command for each additional interface on which you want to prevent fragmented packets.

The following example shows how to configure the fragment database on the outside interface to a maximum size of 2000, a maximum chain length of 45, and a wait time of 10 seconds:

```
ciscoasa(config)# fragment size 2000 outside
ciscoasa(config)# fragment chain 45 outside
ciscoasa(config)# fragment timeout 10 outside
```

The following example displays output from the **show fragment** command that includes the **reassembly virtual** option:

```
ciscoasa(config)# show fragment
Interface: outside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Reassembly: virtual
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

Related Commands

Command	Description
clear configure fragment	Resets all the IP fragment reassembly configurations to defaults.
clear fragment	Clears the operational data of the IP fragment reassembly module.
show fragment	Displays the operational data of the IP fragment reassembly module.
show running-config fragment	Displays the IP fragment reassembly configuration.

frequency

To set the rate at which the selected SLA operation repeats, use the **frequency** command in SLA monitor protocol configuration mode. To restore the default value, use the **no** form of this command.

frequency*seconds*
no frequency

Syntax Description

seconds	The number of seconds between SLA probes. Valid values are from 1 to 604800 seconds. This value cannot be less than the **timeout** value.

Command Default

The default frequency is 60 seconds.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple	
				Context	System
SLA monitor protocol configuration	• Yes	—	• Yes	—	—

Command History

Release	Modification
7.2(1)	This command was added.

Usage Guidelines

An SLA operation repeats at a given frequency for the lifetime of the operation. For example:

- An **ipIcmpEcho** operation with a frequency of 60 seconds repeats by sending the echo request packets once every 60 seconds for the lifetime of the operation.
- The default number of packets in an echo operation is 1. This packet is sent when the operation is started and is then sent again 60 seconds later.

If an individual SLA operation takes longer to execute than the specified frequency value, a statistics counter called “busy” is increased rather than immediately repeating the operation.

The value specified for the **frequency** command cannot be less than the value specified for the **timeout** command.

Examples

The following example configures an SLA operation with an ID of 123 and creates a tracking entry with the ID of 1 to track the reachability of the SLA. The frequency of the SLA operation is set to 3 seconds, and the timeout value is set to 1000 milliseconds.

```
ciscoasa(config)# sla monitor 123
```

```
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time that the SLA operation waits for a response.

fsck

To perform a file system check and to repair corruptions, use the **fsck** command in privileged EXEC mode.

fsck [**/noconfirm**] { **disk0:** | **disk1:** \ | **flash:** }

Syntax Description

/noconfirm	(Optional) Does not prompt for confirmation to repair.
disk0:	Specifies the internal Flash memory, followed by a colon.
disk1:	Specifies the external Flash memory card, followed by a colon.
flash:	Specifies the internal Flash memory, followed by a colon. The **flash** keyword is aliased to **disk0:**.

Command Default

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **fsck** command checks and tries to repair corrupt file systems. Use this command before trying more permanent procedures.

If the FSCK utility fixes an instance of disk corruption (due to a power failure or abnormal shutdown, for example), it creates recovery files named FSCK*xxx* .REC. These files can contain a fraction of a file or a whole file that was recovered while FSCK was running. In rare circumstances, you might need to inspect these files to recover data; generally, these files are not needed, and can be safely deleted.

Note The FSCK utility runs automatically at startup, so you may see these recovery files even if you did not manually enter the **fsck** command.

Examples

The following example shows how to check the file system of the flash memory:

```
ciscoasa# fsck disk0:
```

Related Commands

Command	Description
delete	Removes all user-visible files.
erase	Deletes all files and formats the flash memory.
format	Erases all files on a file system, including hidden system files, and reinstalls the file system.

ftp mode passive

To set the FTP mode to passive, use the ftp mode passive command in global configuration mode. To set the FTP client to active mode, use the **no** form of this command.

ftp mode passive
no ftp mode passive

Command Default

This command is enabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.

Usage Guidelines

The **ftp mode passive** command sets the FTP mode to passive, which is the default. The ASA 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 ASA 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 disables passive mode:

```
ciscoasa(config)# no 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 (Deprecated)

Note The last supported release for this command was Version 8.0(1).

You cannot use the **functions** command for Release 8.0(2). It is deprecated and remains in this command reference only for reasons of backward compatibility. Use the **import** and **export** commands to create URL lists for websites, file access, and plug-ins, customization, and language translations.

To configure automatic downloading of the port forwarding Java applet, Citrix support, file access, file browsing, file server entry, application of a webtype ACL, HTTP proxy, port forwarding, or URL entry over WebVPN for this user or group policy, use the **functions** command in webvpn configuration mode. To remove a configured function, use the **no** form of this command.

functions { **auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none** }
no functions { **auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **port-forward** | **none** }

Syntax Description

auto-download	Enables or disables automatic download of the port forwarding Java applet after 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 ASA 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 ASA 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 ASA. The forwarded proxy modifies the browser's old proxy configuration automatically and redirects all HTTP and HTTPS requests to the new proxy configuration. It supports virtually all client side technologies, including HTML, CSS, JavaScript, VBScript, ActiveX, and Java. The only browser it supports is Microsoft Internet Explorer.
none	Sets a null value for all WebVPN functions. Prevents inheriting functions from a default or specified group policy.

port-forward	Enables port forwarding. When enabled, the ASA uses the port forwarding list defined with the WebVPN **port-forward** command.
url-entry	Enables or disables user entry of URLs. When enabled, the ASA still restricts URLs with any configured URL or network ACLs. When URL entry is disabled, the ASA restricts WebVPN users to the URLs on the home page.

Command Default

Functions are disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was added.
7.1(1)	The **auto-download** and **citrix** keywords were added.
8.0(2)	This command was deprecated.

Usage Guidelines

To remove all configured functions, including a null value created by issuing the **functions none** command, use the **no** form of this command without arguments. The **no** option allows inheritance of a value from another group policy. To prevent inheriting function values, use the **functions none** command.

Examples

The following example shows how to configure file access and file browsing for the group policy named FirstGroup:

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa(config-group-webvpn)# functions file-access file-browsing
```

Related Commands

Command	Description
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.

fxos mode appliance

To set the Firepower 2100 to Appliance mode, use the **fxos mode appliance** command in global configuration mode. To set the mode to Platform mode, use the **no** form of this command.

fxos mode appliance
no fxos mode appliance

Note This command is supported on the Firepower 2100 only.

Syntax Description

This command has no arguments or keywords.

Command Default

The mode is set to Appliance mode by default.

Command Modes

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

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

Command History

Release	Modification
9.13(1)	Command added.

Usage Guidelines

The Firepower 2100 runs an underlying operating system called the FXOS. You can run the Firepower 2100 in the following modes:

- Appliance mode (the default)—Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.
- Platform mode—When in Platform mode, you must configure basic operating parameters and hardware interface settings in FXOS. These settings include enabling interfaces, establishing EtherChannels, NTP, image management, and more. You can use the Firewall Chassis Manager web interface or FXOS CLI. You can then configure your security policy in the ASA operating system using ASDM or the ASA CLI.

When you change the mode, the configuration is cleared and you need to save the current configuration and reload the system. The default configuration is applied upon reload. Prior to reloading, you can set the mode back to the original value without any disruption. Note that the **clear configure all** and **configure factory-default** commands do not clear the current mode.

Use the **show fxos mode** to view the current mode.

Examples

The following example sets the mode to Platform mode:

```
ciscoasa(config)# no fxos mode appliance
Mode set to platform mode
WARNING: This command will take effect after the running-config is saved and the system has
 been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: c0532471 648dc7c2 4f2b4175 1f162684
23736 bytes copied in 1.520 secs (23736 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm]
```

Related Commands

Command	Description
connect fxos	Connects to the FXOS CLI.
show fxos mode	Shows the current mode, Appliance or Platform.

fxos permit

To use FXOS SSH, HTTPS, or SNMP on the Firepower 2100 from an ASA data interface, use the **fxos permit** command in global configuration mode. To disable access, use the **no** form of this command.

fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* } *interface_name*
no fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* } *interface_name*

Syntax Description

https	Allows HTTPS access for the Firewall Chassis Manager. The default port is 3443.
interface_name	Specifies the ASA data interface where access is allowed. You cannot specify a management-only interface.
ipv4_address netmask	Specifies the IPv4 address and subnet mask.
ipv6_address/prefix_length	Specifies the IPv6 prefix and prefix length.
snmp	Allows SNMP access to FXOS. The default port is 3061. For SNMP traffic originating on the device, you must also set the **ip-client** command.
ssh	Allows SSH access to FXOS. The default port is 3022.

Command Default

See the following defaults:

- HTTPS default port—3443
- SNMP default port—3061
- SSH default port—3022

Command Modes

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

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

Command History

Release	Modification
9.8(2)	We added this command.

Usage Guidelines

If you want to manage FXOS on the Firepower 2100 from a data interface, you can configure SSH, HTTPS, and SNMP access. This feature is useful if you want to manage the device remotely, and you want to keep

Management 1/1 on an isolated network. You can continue to use Management 1/1 for local access; you cannot allow remote access from Management 1/1 for FXOS at the same time as forwarding traffic to the ASA data interfaces because you can only specify one gateway. By default, the FXOS management gateway is the internal path to the ASA.

The ASA uses non-standard ports for FXOS access; the standard port is reserved for use by the ASA on the same interface. Use the **fxos port** command to change the port value. When the ASA forwards traffic to FXOS, it translates the non-standard destination port to the FXOS port for each protocol (do not change the HTTPS port in FXOS). The packet destination IP address (which is the ASA interface IP address) is also translated to an internal address for use by FXOS. The source address remains unchanged. For returning traffic, the ASA uses its data routing table to determine the correct egress interface. When you access the ASA data IP address for the management application, you must log in using an FXOS username; ASA usernames only apply for ASA management access.

You can also enable FXOS management traffic initiation on ASA data interfaces using the **ip-client** command, which is required for SNMP traps, or NTP and DNS server access, for example.

In the FXOS configuration, you must configure an access list (**ip-block** command) to allow your management addresses. You need to allow any addresses that you specified in the **fxos permit** commands. Also, make sure the default gateway is set to 0.0.0.0, which sets the ASA as the gateway. See the FXOS **set out-of-band** command.



Note You cannot use a VPN tunnel to an ASA data interface and access FXOS directly. As a workaround for SSH, you can VPN to the ASA, access the ASA CLI, and then use the **connect fxos** command to access the FXOS CLI. Note that SSH, HTTPS, and SNMPv3 are/can be encrypted, so direct connection to the data interface is safe.

Examples

The following example enables SSH and HTTPS access on the inside interface for the 192.168.1.0/24 and 2001:DB8::34/64 networks:

```
ciscoasa(config)# fxos https permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos https permit 2001:DB8::34/64 inside
ciscoasa(config)# fxos ssh permit 192.168.1.0 255.255.155.0 inside
ciscoasa(config)# fxos ssh permit 2001:DB8::34/64 inside
```

Related Commands

Command	Description
connect fxos	From the ASA CLI, connects to the FXOS CLI.
fxos port	Sets the FXOS management access port.
ip-client	Allows FXOS management traffic to egress the ASA data interface.

fxos port

To set the SSH, HTTPS, or SNMP port when accessing FXOS on a Firepower 2100 ASA data interface, use the **fxos port** command in global configuration mode. To use the default port, use the **no** form of this command.

fxos { **https** | **ssh** | **snmp** } **port** *port*
no fxos { **https** | **ssh** | **snmp** } **permit** { *ipv4_address netmask* | *ipv6_address* | *prefix_length* }

Syntax Description

https	Sets the port for HTTPS access for FXOS. The default port is 3443.
port	Specifies the port number.
snmp	Sets the port for SNMP access for FXOS. The default port is 3061.
ssh	Sets the port for SSH access for FXOS. The default port is 3022.

Command Default

See the following defaults:

- HTTPS default port—3443
- SNMP default port—3061
- SSH default port—3022

Command Modes

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

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

Command History

Release	Modification
9.8(2)	We added this command.

Usage Guidelines

When you use the **fxos permit** command to allow FXOS access on a Firepower 2100 data interface, you can set the port to use for each application. The ASA uses non-standard ports for FXOS access; the standard port is reserved for use by the ASA on the same interface. When the ASA forwards traffic to FXOS, it translates the non-standard destination port to the FXOS port for each protocol (do not change the HTTPS port in FXOS).

Examples

The following example sets the ports for SSH and HTTPS access:

```
ciscoasa(config)# fxos https port 6666
ciscoasa(config)# fxos ssh port 7777
```

Related Commands

Command	Description
connect fxos	From the ASA CLI, connects to the FXOS CLI.
fxos permit	Allows FXOS management access on ASA data interfaces.
ip-client	Allows FXOS management traffic to egress the ASA data interface.