CHAPTER 22

file-bookmarks through functions Commands

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).

Defaults

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

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

The default title text is “File Folder Bookmarks”.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

- You can use a comma-separated RGB value, an HTML color value, or the name of the color if recognized in HTML.

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

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

Examples

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

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

Related Commands

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

file-browsing

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

file-browsing enable | disable

Syntax Description

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

Defaults

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The following usage notes apply to file browsing:

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

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

Related Commands

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

file-encoding

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

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

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

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

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

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

Related Commands

Command	Description
character-encoding	Specifies the global character encoding used in all WebVPN portal pages except for pages from servers specified in file encoding entries in the WebVPN configuration.
show running-config 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.

Defaults

No default value or behaviors.

Command Modes

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

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

Command History

Release	Modification
8.0(2)	This command was introduced.

Usage Guidelines

The 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:

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

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

Related Commands

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

filter

To specify the name of the access list to use for WebVPN connections for this group policy or username, use the **filter** command in webvpn configuration mode. To remove the access list, 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.

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

Command	Description
access-list	Creates an access list, or uses a downloadable access list.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn 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.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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:

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

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

Related Commands\

Commands	Description
filter url	Directs traffic to a URL filtering server.
filter java	Removes Java applets from HTTP traffic passing through the 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.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **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:

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

Related Commands

Commands	Description
filter https	Identifies the HTTPS traffic to be filtered by a Websense sor N2H2 erver.
filter java	Removes Java applets from HTTP traffic passing through the 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 foreign_mask* [**allow**]

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

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The 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:

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

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the 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.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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:

```
hostname(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:

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

Related Commands

Commands	Description
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 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.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

```
hostname(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:

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

The following example blocks all outbound HTTP connections destined to a proxy server that listens on port 8080:

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

Related Commands

Commands	Description
filter activex	Removes ActiveX objects from HTTP traffic passing through the 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.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

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

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>
```

Examples

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

```
hostname(config)# fips enable
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing and configuration of crash write info to flash.
fips self-test poweron	Executes power-on self-tests.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(4)	This command was introduced.
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:

```
sw8-5520(config)# fips self-test poweron
```

Related Commands

Command	Description
clear configure fips	Clears the system or module FIPS configuration information stored in NVRAM.
crashinfo console disable	Disables the reading, writing, and configuration of crash write info to Flash.
fips enable	Enables or disablea policy checking to enforce FIPS compliance on the system or module.
show crashinfo console	Reads, writes, and configures crash write to flash.
show running-config fips	Displays the FIPS configuration that is running on the 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.

Defaults

By default, the ASA is in routed mode.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.
8.5(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:

```
hostname(config)# firewall transparent
```

Related Commands

Command	Description
arp-inspection	Enables ARP inspection, which compares ARP packets to static ARP entries.
mac-address-table static	Adds static MAC address entries to the MAC address table.
mac-learn	Disables MAC address learning.
show firewall	Shows the firewall mode.
show mac-address-table	Shows the MAC address table, including dynamic and static entries.

firewall vlan-group (IOS)

To assign VLANs to a firewall group, enter the **firewall vlan-group** command in global configuration mode. To remove the VLANs, use the **no** form of this command.

firewall vlan-group *firewall_group vlan_range*

no firewall vlan-group *firewall_group vlan_range*

Syntax Description

firewall_group	Specifies the group ID as an integer.
vlan_range	Specifies the VLANs assigned to the group. The *vlan_range* can be one or more VLANs (2 to 1000 and from 1025 to 4094) identified in one of the following ways: • A single number (*n*) • A range (*n-x*) Separate numbers or ranges by commas. For example, enter the following numbers: `5,7-10,13,45-100` **Note** Routed ports and WAN ports consume internal VLANs, so it is possible that VLANs in the 1020-1100 range might already be in use.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

In Cisco IOS software, create up to 16 firewall VLAN groups using the **firewall vlan-group** command, and then assign the groups to the ASA (using the **firewall module** command). For example, you can assign all the VLANs to one group, or you can create an inside group and an outside group, or you can create a group for each customer. Each group can contain unlimited VLANs.

You cannot assign the same VLAN to multiple firewall groups; however, you can assign multiple firewall groups to an ASA and you can assign a single firewall group to multiple ASAs. VLANs that you want to assign to multiple ASAs, for example, can reside in a separate group from VLANs that are unique to each ASA.

Examples

The following example shows how you can create three firewall VLAN groups: one for each ASA, and one that includes VLANs assigned to both ASAs.

```
Router(config)# firewall vlan-group 50 55-57
Router(config)# firewall vlan-group 51 70-85
Router(config)# firewall vlan-group 52 100
Router(config)# firewall module 5 vlan-group 50,52
Router(config)# firewall module 8 vlan-group 51,52
```

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group
Group vlans
----- ------
   50 55-57
   51 70-85
   52 100
```

The following is sample output from the **show firewall module** command, which shows all VLAN groups:

```
Router# show firewall module
Module Vlan-groups
  5    50,52
  8    51,52
```

Related Commands

Command	Description
firewall module	Assigns a VLAN group to an ASA.
show firewall vlan-group	Shows the VLAN groups and the VLANs assigned to them.
show module	Shows all installed modules.

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.

Defaults

The default value is 1 minute.

Command Modes

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

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

Command History

Release	Modification
9.1(2)	This command was introduced.

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:

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

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.
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.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
8.1(2)	This command was introduced.

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:

```
hostname(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.
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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	This command was introduced.
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:

```
hostname(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.
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 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.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
8.1(2)	This command was introduced.

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.

```
hostname(config)# access-list flow_export_acl permit ip host 10.1.1.1 host 20.1.1.1
hostname(config)# class-map flow_export_class
hostname(config-cmap)# match access-list flow_export_acl
hostname(config)# policy-map global_policy
hostname(config-pmap)# class flow_export_class
hostname(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.

Defaults

The default value for the interval is 30 minutes.

Command Modes

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

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

Command History

Release	Modification
8.1(1)	This command was introduced.

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:

```
hostname(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.

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.

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. When the buffer usage exceeds the high watermark, 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. After the network interface controller (NIC) sends a pause frame, when the buffer usage is reduced below the low watermark, 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 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 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:

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

Command History

Release	Modification
8.2(2)	This command was introduced 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.

Usage Guidelines

This command is supported on 1-GigabitEthernet and 10-Gigabit Ethernet interfaces. This command does not support management interfaces.

Enter this command for a physical interface.

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

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

1. The NIC sends a pause frame when the buffer usage exceeds the high 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, 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.

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

Examples

The following example enables pause frames using the default settings:

```
hostname(config)# interface tengigabitethernet 1/0
hostname(config-if)# flowcontrol send on
```

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
hostname(config-if)# y
```

Related Commands

Command	Description
interface	Enters interface configuration mode.

format

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

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

Syntax Description

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

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **format** command erases all data on the specified file system and then rewrites the FAT information to the device.

Caution Use the **format** command with extreme caution, only when necessary, to clean up corrupted flash memory.

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

Note On the Cisco 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:

```
hostname# format flash:
```

Related Commands

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

forward interface

For models with a built-in switch, such as the ASA 5505, 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*

Syntax Description

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

Defaults

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

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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.

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

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

Related Commands

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

fqdn (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.

Defaults

The default setting does not include the FQDN.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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:

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

Related Commands

Command	Description
crypto ca trustpoint	Enters crypto ca-trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.
enrollment retry count	Specifies the number of retries to attempt to send an enrollment request.

Command	Description
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.

Defaults

By default, the domain name is an IPv4 domain.

Command Modes

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

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

Command History

Release	Modification
8.4(2)	This command was introduced.

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:

```
hostname (config)# object network FQDN_1
hostname (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.

Defaults

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		
				Multiple	
	Routed	Transparent	Single	Context	System
Global configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was modified so that you now must choose one of the following 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:

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

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

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

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

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

```
hostname(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.

Defaults

The default frequency is 60 seconds.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

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

- An **ipIcmpEcho** operation with a frequency of 60 seconds repeats by sending the echo request packets once every 60 seconds for the lifetime of the operation.
- 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.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
```

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

Related Commands

Command	Description
sla monitor	Defines an SLA monitoring operation.
timeout	Defines the amount of time 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:**.

Defaults

No default behaviors or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **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:

```
hostname# 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 reset the FTP client to active mode, use the **no** form of this command.

ftp mode passive

no ftp mode passive

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ftp mode passive** command sets the FTP mode to passive.The 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 sets the FTP mode to passive:

```
hostname(config)# ftp mode passive
```

Related Commands

copy	Uploads or downloads image files or configuration files to or from an FTP server.
debug ftp client	Displays detailed information about FTP client activity.
show running-config ftp mode	Displays FTP client configuration.

functions

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, customizatioin, and language translations.

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

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

no functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **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.

Defaults

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		
				Multiple	
	Routed	Transparent	Single	Context	System
Webvpn configuration	•	—	•	—	—

Command History

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

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

Related Commands

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