CHAPTER 33

upgrade-mp through xlate-bypass Commands

upgrade-mp

To upgrade the maintenance partition software, use the **upgrade-mp** command.

upgrade-mp {http[**s**]**://**[*user*:*password*@]*server*[:*port*]/*pathname* | **tftp**[**://***server*/*pathname*]}

Syntax Description

tftp	Specifies a TFTP server. If you do not specify the server and path, you are prompted for the information. See the **tftp-server** command to configure a default TFTP server.
http[**s**]	Specifies an HTTP(S) server.
server	Specifies the HTTP(S) or TFTP server IP address.
pathname	Specifies the pathname and filename of the software image.
user	(Optional) Specifies the HTTP(S) username.
password	(Optional) Specifies the user password.
port	(Optional) Specifies the HTTP(S) port.

Defaults

This command has no default settings.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example shows how to download an image from a TFTP server:

```
hostname# upgrade-mp tftp://10.192.1.1/c6svc-mp.2-1-1.bin.gz
```

Related Commands

Command	Description
copy	Copies a file to Flash memory.

uri-non-sip

To identify the non-SIP URIs present in the Alert-Info and Call-Info header fields, use the **uri-non-sip** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

uri-non-sip action {**mask** | **log**} [**log**}

no uri-non-sip action {**mask** | **log**} [**log**}

Syntax Description

mask	Masks the non-SIP URIs.
log	Specifies standalone or additional log in case of violation.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Examples

The following example shows how to identify the non-SIP URIs present in the Alert-Info and Call-Info header fields in a SIP inspection policy map:

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# uri-non-sip action log
```

Related Commands

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

url

To maintain the list of static URLs for retrieving CRLs, use the **url** command in crl configure configuration mode. The crl configure configuration mode is accessible from the crypto ca trustpoint configuration mode. To delete an existing URL, use the **no** form of this command.

url *index url*

no url *index url*

Syntax Description

index	Specifies a value from 1 to 5 that determines the rank of each URL in the list. The FWSM tries the URL at index 1 first.
url	Specifies the URL from which to retrieve the CRL.

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
CRL configure configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You cannot overwrite existing URLs. To replace an existing URL, first delete it using the **no** form of this command.

Examples

The following example enters crl configure configuration mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL https://example.com from which to retrieve CRLs:

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://example.com
hostname(ca-crl)#
```

Related Commands

Command	Description
crl configure	Enters ca-crl configuration mode.
crypto ca trustpoint	Enters trustpoint configuration mode.
policy	Specifies the source for retrieving CRLs.

url-block

To manage the URL buffers used for web server responses while waiting for a filtering decision from the filtering server, use the **url-block** command in global configuration mode. To remove the configuration, use the **no** form of this command.

url-block block *block_buffer_limit*

no url-block block *block_buffer_limit*

Websense only:

url-block url-mempool *memory_pool_size*

no url-block url-mempool *memory_pool_siz*

Syntax Description

block *block_buffer_limit*	Creates an HTTP response buffer to store web server responses while waiting for a filtering decision from the filtering server. In single context mode, the permitted values are from 0 to 128, which specifies the number of 1550-byte blocks. In multiple context mode, the permitted values are from 0 to 16.
url-mempool *memory_pool_size*	For Websense URL filtering only. The size of the URL buffer memory pool in Kilobytes (KB). In single context mode, the permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB. In multiple context mode, the permitted values are from 0 to 512.
url-size *long_url_size*	For Websense URL filtering only. The maximum allowed URL size in KB. The permitted values are 2, 3, or 4, which specifies a maximum URL size of 2 KB, 3 KB, or 4 KB.

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
1.1(1)	This command was introduced.

Usage Guidelines

For Websense filtering servers, the **url-block url-size** command allows filtering of long URLs, up to 4 KB. For both Websense and N2H2 filtering servers, the **url-block block** command causes the FWSM to buffer packets received from a web server in response to a web client request while waiting for a response from the URL filtering server. This improves performance for the web client compared to the default FWSM behavior, which is to drop the packets and to require the web server to retransmit the packets if the connection is permitted.

If you use the **url-block block** command and the filtering server permits the connection, the FWSM sends the blocks to the web client from the HTTP response buffer and removes the blocks from the buffer. If the filtering server denies the connection, the FWSM sends a deny message to the web client and removes the blocks from the HTTP response buffer.

Use the **url-block block command** to specify the number of blocks to use for buffering web server responses while waiting for a filtering decision from the filtering server.

Use the **url-block url-size** command with the **url-block url-mempool** command to specify the maximum length of a URL to be filtered by a Websense filtering server and the maximum memory to assign to the URL buffer. Use these commands to pass URLs longer than 1159 bytes, up to a maximum of 4096 bytes, to the Websense server. The **url-block url-size** command stores URLs longer than 1159 bytes in a buffer and then passes the URL to the Websense server (through a TCP packet stream) so that the Websense server can grant or deny access to that URL.

Examples

The following example assigns 56 1550-byte blocks for buffering responses from the URL filtering server:

```
hostname#(config)# url-block block 56
```

Related Commands

Commands	Description
clear url-block block statistics	Clears the block buffer usage counters.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL block, which is used for buffering URLs while waiting for responses from an N2H2 or Websense 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.

url-cache

To enable URL caching while pending responses from an N2H2 or Websense server and to set the size of the cache, use the **url-cache** command in global configuration mode. To remove the configuration, use the **no** form of this command.

url-cache {**dst** | **src_dst**} *kbytes*[**kb**]

no url-cache {**dst** | **src_dst**} *kbytes*[**kb**]

Syntax Description

dst	Cache entries based on the URL destination address. Select this mode if all users share the same URL filtering policy on the N2H2 or Websense server.
kb	(Optional) Indicates that the size given is in kilobytes. FWSM accepts the **kb** keyword as a convenience in case you add it as a habit.
kbytes	Specifies a value for the cache size within the range 1 to 128 KB.
src_dst	Cache entries based on the both the source address initiating the URL request as well as the URL destination address. Select this mode if users do not share the same URL filtering policy on the N2H2 or Websense server.
statistics	Use the **statistics** option to display additional URL cache statistics, including the number of cache lookups and hit rate.

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
1.1(1)	This command was introduced.

Usage Guidelines

The **url-cache** command provides a configuration option to buffer the response from a web server if its response is faster than that from the N2H2 or Websense filtering service server. This prevents the web server response from being loaded twice.

Use the **url-cache** command to enable URL caching, set the size of the cache, and display cache statistics.

Caching stores URL access privileges in memory on the FWSM. When a host requests a connection, the FWSM first looks in the URL cache for matching access privileges instead of forwarding the request to the N2H2 or Websense server. Disable caching with the **no url-cache** command.

Note If you change settings on the N2H2 or Websense server, disable the cache with the **no url-cache** command and then reenable the cache with the **url-cache** command.

Using the URL cache does not update the Websense accounting logs for Websense protocol Version 1. If you are using Websense protocol Version 1, let Websense run to accumulate logs so that you can view the Websense accounting information. After you get a usage profile that meets your security needs, enable **url-cache** to increase throughput. Accounting logs are updated for Websense protocol Version 4 and for N2H2 URL filtering while using the **url-cache** command.

Examples

The following example caches all outbound HTTP connections based on the source and destination addresses:

```
hostname(config)# url-cache src_dst 128
```

Related Commands

Commands	Description
clear url-cache statistics	Removes **url-cache** command statements from the configuration.
filter url	Directs traffic to a URL filtering server.
show url-cache statistics	Displays information about the URL cache, which is used for buffering URLs while waiting for responses from an N2H2 or Websense 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.

url-server

To identify a smartfilter (formerly N2H2) or Websense server for use with the **filter** command, use the **url-server** command in global configuration mode. To remove the configuration, use the **no** form of this command.

smartfilter (formerly N2H2)

url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

no url-server [<(*if_name*)>] **vendor** {smartfilter | n2h2} **host** <*local_ip*> [**port** <*number*>] [**timeout** <seconds>] [**protocol** {**TCP** [connections <*number*>]} | **UDP**]

Websense

url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | **version 1**|**4**][context-name]

no url-server (*if_name*) **vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | **version 1**|**4**][context-name]

Syntax Description

smartfilter (formerly N2H2)

connections *num_conns*	Indicates number of simultaneous TCP connections established between URL-server and the FWSM. Default value is 5.
host *local_ip*	The server that runs the URL filtering application.
if_name	The network interface where the authentication server resides.
port *number*	The smartfilter (formerly N2H2) server port. The FWSM also listens for UDP replies on this port. The default port number is 4005.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP.
timeout *seconds*	The idle time permitted before the server is marked down and the FWSM switches to the next server, if specified. Default timeout is 30 seconds.
vendor smartfilter (formerly N2H2)	Indicates URL filtering service vendor is **smartfilter** (formerly N2H2).

Websense

connections *num_conns*	Indicates number of simultaneous TCP connections established between URL-server and the FWSM. Default value is 5.
context-name	Sends the context name with each websense query for policy lookups on the websense server. **Note** This feature is available only when websense is configured for filtering [not available with smartfilter (formerly N2H2)], and with websense protocol version 4.0. This feature can be configured only in multiple context mode.
if_name	The network interface where the authentication server resides.
host *local_ip*	The server that runs the URL filtering application.
timeout *seconds*	The idle time permitted before the server is marked down and the FWSM switches to the next server, if specified. Default timeout is 30 seconds.
protocol	The protocol can be configured using **TCP** or **UDP** keywords. The default is TCP protocol, Version 1.
vendor websense	Indicates URL filtering service vendor is Websense.
version	Specifies protocol Version **1** or **4**. The default is TCP protocol Version 1. TCP can be configured using Version 1 or Version 4. UDP can be configured using Version 4 only.

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
1.1(1)	This command was introduced.
4.0	Introduced the **context-name** feature.

Usage Guidelines

The **url-server** command designates the server running the smartfilter (formerly N2H2) or Websense URL filtering application. The limit is 16 URL servers; however, you can use only one application at a time, either smartfilter (formerly N2H2) or Websense. Additionally, changing your configuration on the FWSM does not update the configuration on the application server; this must be done separately, according to the vendor instructions.

The **url-server** command must be configured before issuing the **filter** command for URL, HTTPS and FTP filtering. Before removing all the url-servers from the server list, associated filter commands must be removed.

Once you designate the server, enable the filtering service with the **filter url** command.

To filter URLs, perform the following steps:

Step 1 Designate the URL filtering application server with the appropriate form of the vendor-specific **url-server** command.

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

Step 3 (Optional) Use the **url-cache** command to enable URL caching to improve perceived response time.

Step 4 (Optional) Enable long URL and HTTP buffering support using the **url-block** command.

Step 5 Use the **show url-block block statistics**, **show url-cache statistics**, or the **show url-server statistics** commands to view run information.

For more information about Filtering by smartfilter (formerly N2H2), visit the smartfilter (formerly N2H2) website at:

http://www.n2h2.com

Note The N2H2 corporation was acquired by Secure Computing in October, 2003.

For more information on Websense filtering services, visit the following website:

http://www.websense.com/

Examples

Using smartfilter (formerly N2H2), the following example filters all outbound HTTP connections except those from the 10.0.2.54 host:

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, 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 protocol TCP version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

Using Websense, the following example uses the context-name feature:

```
url-server (inside) host 10.1.1.10 protocol TCP version 4 connections 5 context-name
url-server (inside) host 10.1.1.10 timeout 20 protocol UDP version 4 context-name
```

Related Commands

Commands	Description
show url-server statistics	Shows information about the filtering server and filtering statistics associated with it.
clear url-server statistics	Clears filtering statistics associated with the filtering server.
filter	Directs traffic to the filtering server. In other words, enables filtering.

url-block	For buffering the Content Server Response
url-server	Identifies a smartfilter (formerly N2H2) or Websense server for use with the **filter** command.
url-cache	For caching url-server response. This is allowed, only if websense/smartfilter is configured for it.

user-authentication

To enable user authentication, use the **user-authentication enable** command in group-policy configuration mode. To disable user authentication, use the **user-authentication disable** command. To remove the user authentication attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for user authentication from another group policy.

When enabled, user authentication requires that individual users behind a hardware client authenticate to gain access to the network across the tunnel.

user-authentication {**enable** | **disable**}

no user-authentication

Syntax Description

disable	Disables user authentication.
enable	Enables user authentication.

Defaults

User authentication is disabled.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Individual users authenticate according to the order of authentication servers that you configure.

If you require user authentication on the primary FWSM, be sure to configure it on any backup servers as well.

Examples

The following example shows how to enable user authentication for the group policy named "FirstGroup":

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

Related Commands

Command	Description
ip-phone-bypass	Lets IP phones connect without undergoing user authentication. Secure unit authentication remains in effect.
leap-bypass	Lets LEAP packets from wireless devices behind a VPN client travel across a VPN tunnel prior to user authentication, when enabled. This lets workstations using Cisco wireless access point devices establish LEAP authentication. Then they authenticate again per user authentication.
secure-unit-authentication	Provides additional security by requiring the VPN client to authenticate with a username and password each time the client initiates a tunnel.
user-authentication-idle-timeout	Sets an idle timeout for individual users. If there is no communication activity on a user connection in the idle timeout period, the FWSM terminates the connection.

user-authentication-idle-timeout

To set an idle timeout for individual users behind hardware clients, use the **user-authentication-idle-timeout** command in group-policy configuration mode. To delete the idle timeout value, use the **no** form of this command.

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the idle timeout period. The range is from 1 through 35791394 minutes
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting an user authentication idle timeout value from a default or specified group policy.

Defaults

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**
Group-policy	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

This option allows inheritance of an idle timeout value from another group policy. To prevent inheriting an idle timeout value, use the **user-authentication-idle-timeout none** command.

If there is no communication activity by a user behind a hardware client in the idle timeout period, the FWSM terminates the connection.

The minimum is 1 minute, the default is 30 minutes, and the maximum is 10,080 minutes.

Examples

The following example shows how to set an idle timeout value of 45 minutes for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

Related Commands

Command	Description
user-authentication	Requires users behind hardware clients to identify themselves to the FWSM before connecting.

username

To add a user to the FWSM local database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all usernames, use the **no** version of this command without appending a username.

username {*name*} {**nopassword** | **password** *password* [**encrypted**]} [**privilege** *priv_level*]}

no username [*name*]

Syntax Description

encrypted	Indicates that the password is encrypted. When you define a password in the **username** command, the FWSM encrypts it when it saves it to the configuration for security purposes. When you enter the **show running-config** command, the **username** command does not show the actual password; it shows the encrypted password followed by the **encrypted** keword. For example, if you enter the password "test," the **show running-config** display would appear to be something like the following: `username pat password rvEdRh0xPC8bel7s encrypted` The only time you would actually enter the **encrypted** keyword at the CLI is if you are cutting and pasting a configuration to another FWSM and you are using the same password.
name	Specifies the name of the user as a string from 4 to 15 characters in length.
nopassword	Indicates that this user needs no password.
password *password*	Sets the password as a string from 3 to 16 characters in length.
privilege *priv_level*	Sets a privilege level for this use from 0 to 15 (lowest to highest). The default privilege level is 2. This privilege level is used with command authorization.

Defaults

The default privilege level is 2.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.2(1)	This command was removed from the system execution space. The system now uses the admin context username database where applicable.

Usage Guidelines

The **login** command uses this database for authentication.

If you add users to the local database who can gain access to the CLI and whom you do not want to enter privileged mode, you should enable command authorization. (See the **aaa authorization command** command.) Without command authorization, users can access privileged EXEC mode (and all commands) at the CLI using their own password if their privilege level is 2 or greater (2 is the default). Alternatively, you can use AAA authentication so the user will not be able to use the **login** command, or you can set all local users to level 1 so you can control who can use the **enable** password to access privileged EXEC mode.

You cannot enter the **username** command in the system execution space. However, when you use the **login** command in system, or use Telnet authentication when you session to the FWSM from the switch, the FWSM uses the admin context username database (Telnet authentication for the system execution space is also configured in the admin context).

By default, VPN users that you add with this command have no attributes or group policy association. You must configure all values explicitly using the **username attributes** command.

Examples

The following example shows how to configure a user named "anyuser" with a password of 12345678 and a privilege level of 12:

```
hostname(config)# username anyuser password 12345678 privilege 12
```

Related Commands

Command	Description
clear config username	Clears the configuration for a particular user or for all users.
show running-config username	Displays the running configuration for a particular user or for all users.
username attributes	Enters username attributes mode, which lets you configure AVPs for specific users.

username attributes

To enter the username attributes mode, use the **username attributes** command in username configuration mode. To remove all attributes for a particular user, use the **no** form of this command and append the username. To remove all attributes for all users, use the **no** form of this command without appending a username. The attributes mode lets you configure AVPs for a specified user.

username {*name*} **attributes**

no username [*name*] **attributes**

Syntax Description

name	Provides the name of the user.

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
Username	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The internal user authentication database consists of the users entered with the username command. The login command uses this database for authentication.

The syntax of the commands in attributes mode have the following characteristics in common:

- The **no** form removes the attribute from the running configuration.
- The **none** keyword also removes the attribute from the running configuration. But it does so by setting the attribute to a null value, thereby preventing inheritance.
- Boolean attributes have explicit syntax for enabled and disabled settings.

Examples

The following example shows how to enter username attributes configuration mode for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)#
```

Related Commands

Command	Description
clear config username	Clears the username database.
show running-config username	Displays the running configuration for a particular user or for all users.
username	Adds a user to the FWSM database.

virtual http

To configure a virtual HTTP server, use the **virtual http** command in global configuration mode. To disable the virtual server, use the **no** form of this command.

virtual http *ip_address* [**host** *hostname*] [**warning**]

no virtual http *ip_address* [**host** *hostname*] [**warning**]

Syntax Description

host *hostname*	(Optional) Assigns a hostname to the virtual HTTP server on the FWSM. When a user is forwarded to the virtual HTTP server to enter their AAA username and password, you see the hostname in the following authentication dialog box message: `Username for 'HTTP Authentication (sessionID) from host_name' at server virtual_http_ip` This information helps differentiate the AAA prompt from the destination HTTP server prompt.
ip_address	Sets the IP address for the virtual HTTP server on the FWSM. Make sure this address is an unused address that is routed to the FWSM.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the FWSM. This keyword applies only for text-based browsers, where the redirect cannot happen automatically.

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
1.1(1)	This command was introduced.
3.2(1)	The **host** keyword was added. Direct authentication with the FWSM was added.

Usage Guidelines

This command enables two functions:

- Cascading HTTP authentications—When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM (via a AAA server) and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

This command redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the FWSM. The FWSM prompts for the AAA server username and password. After the AAA server authenticates the user, the FWSM redirects the HTTP connection back to the original server, but it does not include the AAA server username and password. Because the username and password are not included in the HTTP packet, the HTTP server prompts the user separately for the HTTP server username and password.

Note Do not set the **timeout uauth** command duration to 0 seconds when using the **virtual http** command, because this setting prevents HTTP connections to the real web server.

- Direct authentication with the FWSM—You can authenticate directly with the FWSM using the virtual HTTP IP address. Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP(S), Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the FWSM, but want to authenticate other types of traffic, you can configure virtual HTTP; the user connects using HTTP to a given IP address configured on the FWSM, and the FWSM provides an HTTP prompt.

  You must configure authentication for HTTP access to the virtual HTTP address as well as the other services you want to authenticate using the **authentication match** or **aaa authentication include** command.

  When an unauthenticated user connects to the virtual HTTP IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user can successfully access other services that require authentication.

  To log out from the FWSM, reconnect to the virtual HTTP IP address; you are prompted to log out.

Note An HTTPS session through port 443 must also be authenticated before you can log out successfully.

  To use Telnet or SSH instead of HTTP, use the **virtual telnet** or **virtual ssh** command.

Be sure to include the virtual HTTP address as a destination interface in the access list applied to the source interface.

For inbound users (from lower security to higher security), you must add a **static** command for the virtual HTTP IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself). For outbound users, a **static** statement is not required.

Examples

This example shows how to enable virtual HTTP for direct connection along with AAA authentication for other services:

```
hostname(config)# virtual http 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list ACL-IN remark This is the SMTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list ACL-IN remark This is the virtual HTTP address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list AUTH remark This is the SMTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq http
hostname(config)# access-list AUTH remark This is the virtual HTTP address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the FWSM virtual server.
sysopt uauth allow-http-cache	When you enable the **virtual http** command, this command lets you use the username and password in the browser cache to reconnect to the virtual server.
virtual telnet	Provides a virtual Telnet server on the FWSM to let users authenticate with the FWSM before initiating other types of connections that require authentication.

virtual ssh

To configure a virtual SSH server on the FWSM, use the **virtual ssh** command in global configuration mode. To disable the server, use the **no** form of this command. You might need to authenticate users with the virtual SSH server if you require authentication for types of traffic for which the FWSM does not supply an authentication prompt.

virtual ssh *ip_address*

no virtual ssh *ip_address*

Syntax Description

ip_address	Sets the IP address for the virtual SSH server on the FWSM. Make sure this address is an unused address that is routed to the FWSM. For example, if you perform NAT for inside addresses when they access the outside, and you want to provide outside access to the virtual SSH server, you can use one of the global NAT addresses for the virtual SSH server address.

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**
3.2(1)	This command was introduced.

Usage Guidelines

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the FWSM, but want to authenticate other types of traffic, you can configure virtual SSH; the user connects using SSH to a given IP address configured on the FWSM, and the FWSM provides an SSH prompt.

When an unauthenticated user connects to the virtual SSH IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message "Authentication Successful." Then, the user can successfully access other services that require authentication.

To log out from the FWSM, reconnect to the virtual SSH IP address; you are prompted to log out.

To use Telnet or HTTP instead of SSH, use the **virtual telnet** or **virtual http** command.

Examples

The following example shows how to enable virtual SSH along with AAA authentication for other services:

```
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 10.1.2.1 eq telnet
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 209.165.200.225 eq
smtp
hostname(config)# aaa authentication match AUTH inside tacacs+
hostname(config)# virtual ssh 10.1.2.1
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the FWSM virtual server.
virtual http	When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
virtual telnet	Allows users to connect to the FWSM using Telnet to perform authentication for the user.

virtual telnet

To configure a virtual Telnet server on the FWSM, use the **virtual telnet** command in global configuration mode. You might need to authenticate users with the virtual Telnet server if you require authentication for other types of traffic for which the FWSM does not supply an authentication prompt. To disable the server, use the **no** form of this command.

virtual telnet *ip_address*

no virtual telnet *ip_address*

Syntax Description

ip_address	Sets the IP address for the virtual Telnet server on the FWSM. Make sure this address is an unused address that is routed to the FWSM.

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
1.1(1)	This command was introduced.

Usage Guidelines

Although you can configure network access authentication for any protocol or service (see the **aaa authentication match** or **aaa authentication include** command), you can authenticate directly with HTTP, Telnet, or FTP only. A user must first authenticate with one of these services before other traffic that requires authentication is allowed through. If you do not want to allow HTTP, Telnet, or FTP through the FWSM, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the FWSM, and the FWSM provides a Telnet prompt.

You must configure authentication for Telnet access to the virtual Telnet address as well as the other services you want to authenticate using the **authentication match** or **aaa authentication include** command.

When an unauthenticated user connects to the virtual Telnet IP address, the user is challenged for a username and password, and then authenticated by the AAA server. Once authenticated, the user sees the message “Authentication Successful.” Then, the user can successfully access other services that require authentication.

Be sure to include the virtual Telnet address as a destination interface in the access list applied to the source interface.

For inbound users (from lower security to higher security), you must add a **static** command for the virtual Telnet IP address, even if NAT is not required (using the **no nat-control** command). An identity NAT command is typically used (where you translate the address to itself). For outbound users, a **static** statement is not required.

To logout from the FWSM, reconnect to the virtual Telnet IP address; you are prompted to log out.

To use SSH or HTTP instead of Telnet, use the **virtual ssh** or **virtual http** command.

Examples

This example shows how to enable virtual Telnet along with AAA authentication for other services:

```
hostname(config)# virtual telnet 209.165.202.129
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list ACL-IN remark This is the SMTP server on the inside
hostname(config)# access-list ACL-IN extended permit tcp any host 209.165.202.129 eq
telnet
hostname(config)# access-list ACL-IN remark This is the virtual Telnet address
hostname(config)# access-group ACL-IN in interface outside
hostname(config)# static (inside, outside) 209.165.202.129 209.165.202.129 netmask
255.255.255.255
hostname(config)# access-list AUTH extended permit tcp any host 209.165.200.225 eq smtp
hostname(config)# access-list AUTH remark This is the SMTP server on the inside
hostname(config)# access-list AUTH extended permit tcp any host 209.165.202.129 eq telnet
hostname(config)# access-list AUTH remark This is the virtual Telnet address
hostname(config)# aaa authentication match AUTH outside tacacs+
```

Related Commands

Command	Description
clear configure virtual	Removes **virtual** command statements from the configuration.
show running-config virtual	Displays the IP address of the FWSM virtual server.
virtual http	When you use HTTP authentication on the FWSM, and the HTTP server also requires authentication, this command lets you authenticate separately with the FWSM and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the FWSM is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.
virtual ssh	Allows users to connect to the FWSM using SSH to perform authentication for the user.

vpn-access-hours

To associate a group policy with a configured time-range policy, use the **vpn-access-hours** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-range value from another group policy. To prevent inheriting a value, use the **vpn-access-hours none** command.

vpn-access hours value {*time-range*} | **none**

no vpn-access hours

Syntax Description

none	Sets VPN access hours to a null value, thereby allowing no time-range policy. Prevents inheriting a value from a default or specified group policy.
time-range	Specifies the name of a configured time-range policy.

Defaults

Unrestricted.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Examples

The following example shows how to associate the group policy named FirstGroup with a time-range policy called 824:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

Related Commands

Command	Description
time-range	Sets days of the week and hours of the day for access to the network, including start and end dates.

vpn-addr-assign

To specify a method for assigning IP addresses to remote access clients, use the **vpn-addr-assign** command in global configuration mode. To remove the attribute from the configuration, use the **no** form of this command. To remove all configured VPN address assignment methods from the FWSM, user the **no** form of this command without arguments.

vpn-addr-assign {**aaa** | **dhcp** | **local**}

no vpn-addr-assign [**aaa** | **dhcp** | **local**]

Syntax Description

aaa	Obtains IP addresses from an external AAA authentication server.
dhcp	Obtains IP addresses via DHCP.
local	Assigns IP addresses from internal authentication server, and associates them with a tunnel group.

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

If you choose DHCP, you must also use the **dhcp-network-scope** command to define the range of IP addresses that the DHCP server can use.

If you choose local, you must also use the **ip-local-pool** command to define the range of IP addresses to use. You then use the **vpn-framed-ip-address** and **vpn-framed-netmask** commands to assign IP addresses and netmasks to individual users.

If you choose AAA, you obtain IP addresses from either a previously configured RADIUS server.

Examples

The following example shows how to configure DHCP as the address assignment method:

```
hostname(config)# vpn-addr-assign dhcp
```

Related Commands

Command	Description
dhcp-network-scope	Specifies the range of IP addresses the FWSM DHCP server should use to assign addresses to users of a group policy.
ip-local-pool	Creates a local IP address pool.
vpn-framed-ip-address	Specifies the IP address to assign to a particular user.
vpn-framed-ip-netmask	Specifies the netmask to assign to a particular user.

vpn-filter

To specify the name of the access list to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the access list, including a null value created by issuing the **vpn-filter none** command, use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting values, use the **vpn-filter none** command.

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

vpn-filter {**value** *acl_name* | **none**}

no vpn-filter

Syntax Description

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

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
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

Examples

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

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

Related Commands

Command	Description
access-list	Creates an access list.

vpn-framed-ip-address

To specify the IP address to assign to a particular user, use the **vpn-framed-ip-address** command in username mode. To remove the IP address, use the **no** form of this command.

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

Syntax Description

ip_address	Provides the IP address for this user.

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
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Examples

The following example shows how to set an IP address of 10.92.166.7 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

Related Commands

Command	Description
vpn-framed-ip-netmask	Provides the subnet mask for this user.

vpn-framed-ip-netmask

To specify the subnet mask to assign to a particular user, use the **vpn-framed-ip-netmask** command in username mode. To remove the subnet mask, use the **no** form of this command.

vpn-framed-ip-netmask {*netmask*}

no vpn-framed-ip-netmask

Syntax Description

netmask	Provides the subnet mask for this user.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Examples

The following example shows how to set a subnet mask of 255.255.255. 254 for a user named anyuser:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
```

Related Commands

Command	Description
vpn-framed-ip-address	Provides the IP address for this user.

vpn-group-policy

To have a user inherit attributes from a configured group policy, use the **vpn-group-policy** command in username configuration mode. To remove a group policy from a user configuration, use the **no** version of this command. Using this command lets users inherit attributes that you have not configured at the username level.

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

Syntax Description

group-policy name	Provides the name of the group policy.

Defaults

By default, VPN users have no group policy association.

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**
Username attributes configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	Support for this command was introduced.

Usage Guidelines

You can override the value of an attribute in a group policy for a particular user by configuring it in username mode, if that attribute is available in username mode.

Examples

The following example shows how to configure a user named anyuser to use attributes from the group policy named FirstGroup:

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

Related Commands

Command	Description
group-policy	Adds a group policy to the FWSM database.
group-policy attributes	Enters group-policy attributes mode, which lets you configure AVPs for a group policy.

Command	Description
username	Adds a user to the FWSM database.
username attributes	Enters username attributes mode, which lets you configure AVPs for specific users.

vpn-idle-timeout

To configure a user timeout period use the **vpn-idle-timeout** command in group-policy configuration mode or in username configuration mode. If there is no communication activity on the connection in this period, the FWSM terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-idle-timeout none** command.

vpn-idle-timeout {*minutes* | **none**}

no vpn-idle-timeout

Syntax Description

minutes	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
none	Permits an unlimited idle timeout period. Sets idle timeout with a null value, thereby disallowing an idle timeout. Prevents inheriting a value from a default or specified group policy.

Defaults

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
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example shows how to set a VPN idle timeout of 15 minutes for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-session-timeout	Configures the maximum amount of time allowed for VPN connections. At the end of this period of time, the FWSM terminates the connection.

vpn-sessiondb logoff

To log off all or selected VPN sessions, use the **vpn-sessiondb logoff** command in global configuration mode.

vpn-sessiondb logoff {**remote** | **l2l** | **email-proxy** | **protocol** *protocol-name* | **name** *username* | **ipaddress** *IPaddr* | **tunnel-group** *groupname* | **index** *indexnumber* | **all**}

Syntax Description

all	Logs off all VPN sessions.
email-proxy	Logs off all e-mail proxy sessions.
index *indexnumber*	Logs off a single session by index number. Specify the index number for the session.
ipaddress *IPaddr*	Logs off sessions for the IP address that you specify.
l2l	Logs off all LAN-to-LAN sessions.
name *username*	Logs off sessions for the username that you specify.
protocol *protocol-name*	Logs off sessions for protocols that you specify. The protocols include: IKE POP3S IMAP4S SMTPS IPSec userHTTPS IPSecLAN2LAN vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	Logs off all remote-access sessions.
tunnel-group *groupname*	Logs off sessions for the tunnel group that you specify.

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
3.1(1)	Support for this command was introduced.

Examples

The following example shows how to log off all remote-access sessions:

```
hostname# vpn-sessiondb logoff remote
```

The following example shows how to log off all IPSec sessions:

```
hostname# vpn-sessiondb logoff protocol IPSec
```

vpn-sessiondb max-session-limit

To limit VPN sessions to a lower value than the FWSM allows, use the **vpn-sessiondb max-session-limit** command in global configuration mode. To remove the session limit, use the **no** form of this command. To overwrite the current setting, use the command again.

vpn-sessiondb max-session-limit {*session-limit*}

no vpn-sessiondb max-session-limit

Syntax Description

session-limit	Specifies the maximum number of VPN sessions permitted.

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
3.1(1)	Support for this command was introduced.

Usage Guidelines

This command applies to all types of VPN sessions, including WebVPN.

Examples

The following example shows how to set a maximum VPN session limit of 450:

```
hostname# vpn-sessiondb max-session-limit 450
```

vpn-session-timeout

To configure a maximum amount of time allowed for VPN connections, use the **vpn-session-timeout** command in group-policy configuration mode or in username configuration mode. At the end of this period of time, the FWSM terminates the connection.

To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a time-out value from another group policy. To prevent inheriting a value, use the **vpn-session-timeout none** command.

vpn-session-timeout {*minutes* | **none**}

no vpn-session-timeout

Syntax Description

minutes	Specifies the number of minutes in the timeout period. Use an integer between 1 and 35791394.
none	Permits an unlimited session timeout period. Sets session timeout with a null value, thereby disallowing a session timeout. Prevents inheriting a value from a default or specified group policy.

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
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example shows how to set a VPN session timeout of 180 minutes for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

Related Commands

group-policy	Creates or edits a group policy.
vpn-idle-timeout	Configures the user timeout period. If there is no communication activity on the connection in this period, the FWSM terminates the connection.

vpn-simultaneous-logins

To configure the number of simultaneous logins permitted for a user, use the **vpn-simultaneous-logins** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value from another group policy. Enter 0 to disable login and prevent user access.

vpn-simultaneous-logins {*integer*}

no vpn-simultaneous-logins

Syntax Description

integer	A number between 0 and 2147483647.

Defaults

The default is 3 simultaneous logins.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Enter 0 to disable login and prevent user access.

Examples

The following example shows how to allow a maximum of 4 simultaneous logins for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

To configure a VPN tunnel type (IPSec), use the **vpn-tunnel-protocol** command in group-policy configuration mode or username configuration mode. To remove the attribute from the running configuration, use the **no** form of this command.

vpn-tunnel-protocol IPSec

no vpn-tunnel-protocol [IPSec]

Syntax Description

IPSec	Negotiates an IPSec tunnel between two peers (a remote access client or another secure gateway). Creates security associations that govern authentication, encryption, encapsulation, and key management.
webvpn	Provides VPN services to remote users via an HTTPS-enabled web browser, and does not require a client.

Defaults

IPSec.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	Routed	Transparent	Single	Context	System
Group-policy	•	•	•	•	—
Username	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use this command to configure one or more tunneling modes. You must configure at least one tunneling mode for users to connect over a VPN tunnel.

Examples

The following example shows how to configure IPSec tunneling modes for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

who

To display active Telnet administration sessions on the FWSM, use the **who** command in privileged EXEC mode.

who [*local_ip*]

Syntax Description

local_ip	(Optional) Specifies to limit the listing to one internal IP address or network address, either IPv4 or IPv6.

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
1.1(1)	This command was introduced.

Usage Guidelines

The **who** command allows you to display the TTY_ID and IP address of each Telnet client that is currently logged into the FWSM.

Examples

The following example shows the output of the **who** command when a client is logged into the FWSM through a Telnet session:

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

Related Commands

Command	Description
kill	Terminate a Telnet session.
telnet	Adds Telnet access to the FWSM console and sets the idle timeout.

wins-server

To set the IP address of the primary and secondary WINS servers, use the **wins-server** command in group-policy configuration mode. To remove the attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a WINS server from another group policy. To prevent inheriting a server, use the **wins-server none** command.

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

Syntax Description

none	Sets wins-servers to a null value, thereby allowing no WINS servers. Prevents inheriting a value from a default or specified group policy.
value *ip_address*	Specifies the IP address of the primary and secondary WINS servers.

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
Group-policy	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Every time you issue the **wins-server** command you overwrite the existing setting. For example, if you configure WINS server x.x.x.x and then configure WINS server y.y.y.y, the second command overwrites the first, and y.y.y.y becomes the sole WINS server. The same holds true for multiple servers. To add a WINS server rather than overwrite previously configured servers, include the IP addresses of all WINS servers when you enter this command.

Examples

The following example shows how to configure WINS servers with the IP addresses 10.10.10.15, 10.10.10.30, and 10.10.10.45 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

To erase the startup configuration, use the **write erase** command in privileged EXEC mode. The running configuration remains intact.

write erase

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is not supported within a security context. Context startup configurations are identified by the **config-url** command in the system configuration. If you want to delete a context configuration, you can remove the file manually from the remote server (if specified) or clear the file from Flash memory using the **delete** command in the system execution space.

Examples

The following example erases the startup configuration:

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
delete	Removes a file from Flash memory.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

write memory

To save the running configuration to the startup configuration, use the **write memory** command in privileged EXEC mode.

write memory [**all** [**/noconfirm**]]

Syntax Description

/noconfirm	Eliminates the confirmation prompt when you use the **all** keyword.
all	From the system execution space in multiple context mode, this keyword saves all context configurations as well as the system configuration.

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
1.1(1)	This command was introduced.
3.1(1)	You can now save all context configurations with the **all** keyword.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line. Changes are only preserved between reboots if you save them to the startup configuration, which is the configuration loaded into running memory at startup. The startup configuration for single context mode and for the system in multiple context mode is a hidden file. For multiple context mode, a context startup configuration is at the location specified by the **config-url** command in the system configuration.

In multiple context mode, you can enter the **write memory** command in each context to save the current context configuration. To save all context configurations, enter the **write memory all** command in the system execution space. Context startup configurations can reside on external servers. In this case, the FWSM saves the configuration back to the server specified by the **config-url** command, except for HTTP and HTTPS URLs, which do not allow you to save the configuration back to the server. After the FWSM saves each context with the **write memory all** command, the following message appears:

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

Sometimes, a context is not saved because of an error. See the following information for errors:

- For contexts that are not saved because of low memory, the following message appears:

```
The context 'context a' could not be saved due to Unavailability of resources
```

- For contexts that are not saved because the remote destination is unreachable, the following message appears:

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- For contexts that are not saved because the context is locked, the following message appears:

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context ‘a’ , context ‘x’ , context ‘z’ .
  ```

  A context is only locked if another user is already saving the configuration or in the process of deleting the context.

- For contexts that are not saved because the startup configuration is read-only (for example, on an HTTP server), the following message report is printed at the end of all other messages:

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context ‘a’ , context ‘b’ , context ‘c’ .
  ```

- For contexts that are not saved because of bad sectors in the Flash memory, the following message appears:

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

Because the system uses the admin context interfaces to access context startup configurations, the **write memory** command also uses the admin context interfaces. The **write net** command, however, uses the context interfaces to write a configuration to a TFTP server.

The **write memory** command is equivalent to the **copy running-config startup-config** command.

Examples

The following example saves the running configuration to the startup configuration:

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

Related Commands

Command	Description
admin-context	Sets the admin context.
configure memory	Merges the startup configuration with the running configuration.
config-url	Specifies the location of the context configuration.
copy running-config startup-config	Copies the running configuration to the startup configuration.
write net	Copies the running configuration to a TFTP server.

write net

To save the running configuration to a TFTP server, use the **write net** command in privileged EXEC mode.

write net [*server***:**[*filename*] | **:***filename*]

Syntax Description

:*filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional. If you specify the filename in this command as well as a name in the **tftp-server** command, the FWSM treats the **tftp-server** command filename as a directory, and adds the **write net** command filename as a file under the directory. To override the **tftp-server** command value, enter a slash in front of the path and filename. The slash indicates that the path is not relative to the tftpboot directory, but is an absolute path. The URL generated for this file includes a double slash (//) in front of the filename path. If the file you want is in the tftpboot directory, you can include the path for the tftpboot directory in the filename path. If your TFTP server does not support this type of URL, use the **copy running-config tftp** command instead. If you specified the TFTP server address using the **tftp-server** command, you can enter the filename alone preceded by a colon (:).
*server***:**	Sets the TFTP server IP address or name. This address overrides the address you set in the **tftp-server** command, if present. The default gateway interface is the highest security interface; however, you can set a different interface name using the **tftp-server** command.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The running configuration is the configuration currently running in memory, including any changes you made at the command line.

In multiple context mode, this command saves only the current configuration; you cannot save all contexts with a single command. You must enter this command separately for the system and for each context. The **write net** command uses the context interfaces to write a configuration to a TFTP server. The **write memory** command, however, uses the admin context interfaces to save to the startup configuration because the system uses the admin context interfaces to access context startup configurations.

The **write net** command is equivalent to the **copy running-config tftp** command.

Examples

The following example sets the TFTP server and filename in the **tftp-server** command:

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command is not populated.

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

The following example sets the server and filename in the **write net** command. The **tftp-server** command supplies the directory name, and the server address is overridden.

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
copy running-config tftp	Copies the running configuration to a TFTP server.
show running-config	Shows the running configuration.
tftp-server	Sets a default TFTP server and path for use in other commands.
write memory	Saves the running configuration to the startup configuration.

write standby

To copy the FWSM or context running configuration to the failover standby unit, use the **write standby** command in privileged EXEC mode.

write standby

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines

For Active/Standby failover, the **write standby** command writes the configuration stored in the RAM of the active failover unit to the RAM on the standby unit. Use the **write standby** command if the primary and secondary unit configurations have different information. Enter this command on the active unit.

For Active/Active failover, the **write standby** command behaves as follows:

- If you enter the **write standby** command in the system execution space, the system configuration and the configurations for all of the security contexts on the FWSM is written to the peer unit. This includes configuration information for security contexts that are in the standby state. You must enter the command in the system execution space on the unit that has failover group 1 in the active state.
- If you enter the **write standby** command in a security context, only the configuration for the security context is written to the peer unit. You must enter the command in the security context on the unit where the security context appears in the active state.

Note The **write standby** command replicates the configuation to the running configuration of the peer unit; it does not save the configuration to the startup configuration. To save the configuration changes to the startup configuration, use the **copy running-config startup-config** command on the same unit that you entered the **write standby** command. The command will be replicated to the peer unit and the configuration saved to the startup configuration.

Examples

The following example writes the current running configuration to the standby unit:

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

Related Commands

Command	Description
failover reload-standby	Forces the standby unit to reboot.

write terminal

To show the running configuration on the terminal, use the **write terminal** command in privileged EXEC mode.

write terminal

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

This command is equivalent to the **show running-config** command.

Examples

The following example writes the running configuration to the terminal:

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

Related Commands

Command	Description
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.
write memory	Saves the running configuration to the startup configuration.

xlate-bypass

To disable NAT sessions for untranslated traffic, use the **xlate-bypass** command in global configuration mode. To disable xlate bypass, use the **no** form of this command.

xlate-bypass

no xlate-bypass

Syntax Description

This command has no arguments or keywords.

Defaults

Xlate bypass 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
3.2(1)	This command was introduced.

Usage Guidelines

By default, the FWSM creates NAT sessions for all connections even if you do not use NAT. For example, a session is created for each untranslated connection even if you do not enable NAT control, you use NAT exemption or identity NAT, or you use same security interfaces and do not configure NAT. Because there is a maximum number of NAT sessions (see the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide*), these kinds of NAT sessions might cause you to run into the limit.

To avoid running into the limit, you can disable NAT sessions for untranslated traffic using the **xlate-bypass** command. If you disable NAT control and have untranslated traffic or use NAT exemption, or you enable NAT control (using the **nat-control** command) and use NAT exemption, then with xlate bypass, the FWSM does not create a session for these types of untranslated traffic. NAT sessions are still created in the following instances:

- You configure identity NAT (with or without NAT control). Identity NAT is considered to be a translation.
- You use same-security interfaces with NAT control. Traffic between same security interfaces create NAT sessions even when you do not configure NAT for the traffic. To avoid NAT sessions in this case, disable NAT control or use NAT exemption as well as xlate bypass.
- You configure xlate bypass when the NAT statement has the TCP/UDP max-conn-limit set, which is not the default.

Examples

The following example enables xlate bypass:

```
hostname(config)# xlate-bypass
```

Related Commands

Command	Description
nat	Configures NAT.
nat-control	Enables NAT control.
same-security-traffic inter-interface	Allows interfaces on the same security level to communicate.
show running-config xlate-bypass	Shows the xlate bypass configuration.
show xlate	Shows current translation and connection information.