C H A P T E R **33**

urgent-flag through write terminal Commands

urgent-flag

To allow or clear the URG pointer through the TCP normalizer, use the **urgent-flag** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

Syntax Description	**allow**	Allows the URG pointer through the TCP normalizer.
	clear	Clears the URG pointer through the TCP normalizer.

Defaults The urgent flag and urgent offset are clear by default.

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

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

Command History	**Release**	**Modification**
	7.0(1)	This command was introduced.

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **urgent-flag** command in tcp-map configuration mode to allow the urgent flag.

The URG flag is used to indicate that the packet contains information that is of higher priority than other data within the stream. The TCP RFC is vague about the exact interpretation of the URG flag, therefore, end systems handle urgent offsets in different ways, which may make the end system vulnerable to attacks. The default behavior is to clear the URG flag and offset.

Examples The following example shows how to allow the urgent flag:

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 513
hostname(config)# policy-map pmap
```

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

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

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 security appliance 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
	7.0(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 ca-crl configuration mode, and sets up an index 3 for creating and maintaining a list of URLs for CRL retrieval and configures the URL https://foobin.com from which to retrieve CRLs:

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

The **url-block** commands can be used to manage the URL buffers used for web server responses while waiting for a filtering decision from the filtering server. The **url-block** commands are also used to manage filtering of long URLs. 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*

The numeric parameters for the **url-block** command are lower in multi-context mode than in single-context mode. For example:

Single-context:

> **url-block block** *block_buffer_limit*—max is 128
>
> **url-block url-mempool** *memory_pool_size*—max is 10240

Multi-context:

> **url-block block** *block_buffer_limit*—max is 16
>
> **url-block url-mempool** *memory_pool_size*—max is 512

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. The permitted values are from 0 to 128, which specifies the number of 1550-byte blocks.
	url-mempool *memory_pool_size*	For Websense URL filtering only. The size of the URL buffer memory pool in Kilobytes (KB). The permitted values are from 2 to 10240, which specifies a URL buffer memory pool from 2 KB to 10240 KB.
		✎ **Note** This is not supported on the UDP transport servers.
	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 4KB.
		✎ **Note** This is not supported on the UDP transport servers.

Defaults   This command is disabled by default.

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines   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 security appliance 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 security appliance 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 security appliance 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 security appliance 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 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-cache

To enable URL caching for URL responses received 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.
size *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
	Preexisting	This command was preexisting.

Usage Guidelines   The **url-cache** command provides a configuration option to cache responses from the URL server.

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 security appliance. When a host requests a connection, the security appliance 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 re-enable 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 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 URL responses received from an N2H2 or Websense filtering server.
url-server	Identifies an N2H2 or Websense server for use with the **filter** command.

url-list

To configure a set of URLs for WebVPN users to access, use the **url-list** command in global configuration mode. To configure a list with multiple URLs, use this command with the same listname multiple times, once for each URL. To remove an entire configured list, use the **no url-list** *listname* command. To remove a configured URL, use the **no url-list** *listname url* command.

To configure multiple lists, use this command multiple times, assigning a unique *listname* to each list.

    url-list {*listname displayname url*}

    no url-list *listname*

    no url-list *listname url*

Syntax Description

displayname	Provides the text that displays on the WebVPN end user interface to identify the URL. Maximum 64 characters. The *displayname* must be unique for a given list. Spaces are allowed.
listname	Groups the set of URLs that WebVPN users can access. Maximum 64 characters. Maximum 64 characters. Semi-colons (;) ampersands (&), and less-than (<) characters are not allowed.
url	Specifies the link. Supported URL types are http, https and cifs.

Defaults   There is no default URL list.

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 mode	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines   You use the url-list command in global configuration mode to create one or more lists of URLs. To allow access to the URLs in a list for a specific group policy or user, use the *listname* you create here with the **url-list** command in webvpn mode.

■ **url-list**

Examples   The following example shows how to create a URL list called *Marketing URLs* that provides access to www.cisco.com, www.example.com, and www.example.org. The following table provides values that the example uses for each application.

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

Related Commands

Command	Description
clear configuration url-list	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
url-list	Use this command in webvpn mode to permit a group policy or user to access a previously configured list of urls.
show running-configuration url-list	Displays the current set of configured urls.
webvpn	Use in group-policy configuration mode or in username configuration mode. Lets you enter webvpn mode to configure parameters that apply to group policies or usernames.
webvpn	Use in global configuration mode. Lets you configure global settings for WebVPN.

url-list (webvpn)

To apply a list of WebVPN servers and URLs to a particular user or group policy, use the **url-list** command in group-policy webvpn configuration mode or in username webvpn configuration mode. To remove a list, including a null value created by using the **url-list none command,** use the **no** form of this command. The **no** option allows inheritance of a value from another group policy. To prevent inheriting a url list, use the **url-list none** command. Using the command a second time overrides the previous setting.

> **url-list** {**value** *name* | **none**} [*index*]

> **no url-list**

Syntax Description

index	Indicates the display priority on the home page.
none	Sets a null value for url lists. Prevents inheriting a list from a default or specified group policy.
value *name*	Specifies the name of a previously configured list of urls. To configure such a list, use the **url-list** command in global configuration mode.

Defaults

There is no default URL list.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Using the command a second time overrides the previous setting.

Before you can use the **url-list** command in webvpn mode to identify a URL list that you want to display on the WebVPN home page for a user or group policy, you must create the list. Use the **url-list** command in global configuration mode to create one or more lists.

Examples

The following example applies a URL list called FirstGroupURLs for the group policy named FirstGroup and assigns it first place among the URL lists:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
```

Related Commands

Command	Description
clear configure url-list [*listname*]	Removes all url-list commands from the configuration. If you include the listname, the security appliance removes only the commands for that list.
show running-configuration url-list	Displays the current set of configured **url-list** commands.
url-list	Use this command in webvpn mode, which you access in global configuration mode, to configure the set of URLs that WebVPN users can access.
webvpn	Lets you enter webvpn mode. This can be webvpn configuration mode, group-policy webvpn configuration mode (to configure webvpn settings for a specific group policy), or username webvpn configuration mode (to configure webvpn settings for a specific user).

url-server

To identify an 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.

N2H2

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

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

Websense

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

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

Syntax Description   **N2H2**

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.
if_name	(Optional) The network interface where the authentication server resides. If not specified, the default is inside.
port *number*	The N2H2 server port. The security appliance 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 maximum idle time permitted before the security appliance switches to the next server you specified. The default is 30 seconds.
vendor n2h2	Indicates URL filtering service vendor is N2H2.

Websense

connections	Limits the maximum number of TCP connections permitted.
num_conns	Specifies the maximum number of TCP connections created from the security appliance to the URL server. Since this number is per server, different servers can have different connection values.
host *local_ip*	The server that runs the URL filtering application.
if_name	The network interface where the authentication server resides. If not specified, the default is inside.

timeout *seconds*	The maximum idle time permitted before the security appliance switches to the next server you specified. The default 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 |
| Preexisting | This command was preexisting. |

Usage Guidelines   The **url-server** command designates the server running the N2H2 or Websense URL filtering application. The limit is 16 URL servers in single context mode and 4 URL servers in multi mode; however, and you can use only one application at a time, either N2H2 or Websense. Additionally, changing your configuration on the security appliance 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 HTTPS and FTP. If all URL servers are removed from the server list, then all **filter** commands related to URL filtering are also removed.

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

Use the **show url-server statistics** command to view server statistic information including unreachable servers.

Follow these steps to filter URLs:

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 N2H2, visit N2H2's website at:

http://www.n2h2.com

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

http://www.websense.com/

Examples   Using 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) vendor websense 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
```

Related Commands

Commands	Description
clear url-server	Clears the URL filtering server statistics.
filter url	Directs traffic to a URL filtering server.
show url-block	Displays information about the URL cache, which is used for URL responses received 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.

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
7.0(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 security appliance, 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 security appliance 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. 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 security appliance terminates the connection.

> **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
7.0(1)	This command was introduced.

Usage Guidelines   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 security appliance before connecting.

■ **username**

username

To add a user to the security appliance 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.
name	Provides the name of the user.
nopassword	Indicates that this user needs no password.
password *password*	Indicates that this user has a password, and provides the password.
privilege *priv_level*	Sets a privilege level for this user. The range is from 0 to 15, with lower numbers having less ability to use commands and administer the security appliance. The default privilege level is 2. The typical privilege level for a system administrator is 15.

Defaults

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

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

Use the **username attributes** command to enter config-username mode, in which you can configure any of the following attributes:

Attribute	Function
group-lock	Name an existing tunnel-group with which the user is required to connect.
password-storage	Enables/disables storage of the login password on the client system.
vpn-access-hours	Specifies the name of a configured time-range policy.
vpn-filter	Specifies the name of a user-specific ACL
vpn-framed-ip-address	Specifies the IP address and the net mask to be assigned to the client.
vpn-group-policy	Specifies the name of a group-policy from which to inherit attributes.
vpn-idle-timeout	Specifies the idle timeout period in minutes, or **none** to disable.
vpn-session-timeout	Specifies the maximum user connection time in minutes, or **none** for unlimited time.
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed.
vpn-tunnel-protocol	Specifies permitted tunneling protocols.
webvpn	Enters webvpn mode, in which you configure webvpn attributes.

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

```
hostname(config)# username anyuser password 12345678 encrypted 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 attributes for specific users.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

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 Attribute-Value Pairs 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
7.0.1	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. You can configure the username attributes using either the **username** command or the **username attributes** command.

The syntax of the commands in config-username 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.

The **username attributes** command enters config-username mode, in which you can configure any of the following attributes:

Attribute	Function
group-lock	Name an existing tunnel-group with which the user is required to connect.
password-storage	Enables/disables storage of the login password on the client system.
vpn-access-hours	Specifies the name of a configured time-range policy.
vpn-filter	Specifies the name of a user-specific ACL
vpn-framed-ip-address	Specifies the IP address and the net mask to be assigned to the client.
vpn-group-policy	Specifies the name of a group-policy from which to inherit attributes.
vpn-idle-timeout	Specifies the idle timeout period in minutes, or **none** to disable.
vpn-session-timeout	Specifies the maximum user connection time in minutes, or **none** for unlimited time.
vpn-simultaneous-logins	Specifies the maximum number of simultaneous logins allowed.
vpn-tunnel-protocol	Specifies permitted tunneling protocols.
webvpn	Enters webvpn mode, in which you configure webvpn attributes.

You configure webvpn-mode attributes for the username by entering the **username attributes** command and then entering the **webvpn** command in username webvpn configuration mode. See the description of the **webvpn** command (group-policy attributes and username attributes modes) for details.

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 security appliance database.
webvpn	Enters username webvpn configuration mode, in which you can configure the WebVPN attributes for the specified group.

username-prompt

To customize the username prompt of the WebVPN page login box that is displayed to WebVPN users when they connect to the security appliance, use the **username-prompt** command from webvpn customization mode:

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

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

Syntax Description		
text	Specifies you are changing the text.
style	Specifies you are changing the style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default is text of the username prompt is "USERNAME:".

The default style of the username prompt is color:black;font-weight:bold;text-align:right.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

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

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

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

Examples   In the following example, the text is changed to "Corporate Username:", and the default style is changed with the font weight increased to bolder:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# username-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# username-prompt style font-weight:bolder
```

Related Commands

Command	Description
group-prompt	Customizes the group prompt of the WebVPN page.
password-prompt	Customizes the password prompt of the WebVPN page.

user-parameter

To specify the name of the HTTP POST request parameter in which a username must be submitted for SSO authentication, use the **user-parameter** command in aaa-server-host configuration mode. This is an SSO with HTTP Forms command.

> **user-parameter** *name*

✎
Note   To configure SSO with the HTTP protocol correctly, you must have a thorough working knowledge of authentication and HTTP protocol exchanges.

Syntax Description

string	The name of the username parameter included in the HTTP POST request. The maximum name size is 128 characters.

Defaults   There is no default value or behavior.

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
Aaa-server-host configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines   The WebVPN server of the security appliance uses an HTTP POST request to submit a single sign-on authentication request to an SSO server. The required command **user-parameter** specifies that the HTTP POST request must include a username parameter for SSO authentication.

✎
Note   At login, the user enters the actual name value which is entered into the HTTP POST request and passed on to the authenticating web server.

Examples   The following example, entered in aaa-server-host configuration mode, specifies that the username parameter userid be included in the HTTP POST request used for SSO authentication:

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

	Command	Description
Related Commands	**action-uri**	Specifies a web server URI to receive a username and password for single sign-on authentication.
	auth-cookie-name	Specifies a name for the authentication cookie.
	hidden-parameter	Creates hidden parameters for exchange with the authenticating web server.
	password-parameter	Specifies the name of the HTTP POST request parameter in which a user password must be submitted for SSO authentication.
	start-url	Specifies the URL at which to retrieve a pre-login cookie.

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. When you use HTTP authentication on the security appliance, and the HTTP server also requires authentication, this command allows you to authenticate separately with the security appliance and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.

virtual http *ip_address* [**warning**]

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

Syntax Description

ip_address	Sets the IP address for the virtual HTTP server on the security appliance. Make sure this address is an unused address that is routed to the security appliance. For example, if you perform NAT for inside addresses when they access the outside, and you want to provide outside access to the virtual HTTP server, you can use one of the global NAT addresses for the virtual HTTP server address.
warning	(Optional) Notifies users that the HTTP connection needs to be redirected to the security appliance. 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
Preexisting	This command was preexisting.

Usage Guidelines   If you enable HTTP authentication (see the **aaa authentication match** command or the **aaa authentication include** command), then the security appliance prompts each user for a username and password so it can authenticate them with a AAA server. After the AAA server authenticates the user, the connection is allowed to continue to the HTTP server. However, the AAA server username and password is still included in the HTTP packet. If the HTTP server also has its own authentication mechanism, then the user is not prompted again for a username and password because there is already a username and password included in the packet. Assuming the username and password is not the same for the AAA and HTTP servers, then the HTTP authentication fails.

To allow a user to be prompted separately by the HTTP server, enable the virtual HTTP server on the security appliance using the **virtual http** command. This command redirects all HTTP connections that require AAA authentication to the virtual HTTP server on the security appliance. The security appliance prompts for the AAA server username and password. After the AAA server authenticates the user, the security appliance 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.

⚠

Caution   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.

Examples   This example shows how to enable virtual HTTP along with AAA authentication:

```
hostname(config)# access-list HTTP-ACL extended permit tcp 10.1.1.0 any eq 80
hostname(config)# aaa authentication match HTTP-ACL inside tacacs+
hostname(config)# virtual http 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 security appliance 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 security appliance to let users authenticate with the security appliance before initiating other types of connections that require authentication.

virtual telnet

To configure a virtual Telnet server on the security appliance, 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 security appliance 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 security appliance. Make sure this address is an unused address that is routed to the security appliance. For example, if you perform NAT for inside addresses when they access the outside, and you want to provide outside access to the virtual Telnet server, you can use one of the global NAT addresses for the virtual Telnet 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
Preexisting	This command was preexisting.

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 security appliance, but want to authenticate other types of traffic, you can configure virtual Telnet; the user Telnets to a given IP address configured on the security appliance, and the security appliance provides a Telnet prompt.

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.

Examples   This example shows how to enable virtual Telnet 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 telnet 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 security appliance virtual server.
virtual http	When you use HTTP authentication on the security appliance, and the HTTP server also requires authentication, this command allows you to authenticate separately with the security appliance and with the HTTP server. Without virtual HTTP, the same username and password you used to authenticate with the security appliance is sent to the HTTP server; you are not prompted separately for the HTTP server username and password.

vlan

To assign a VLAN ID to a subinterface, use the **vlan** command in interface configuration mode. To remove a VLAN ID, use the **no** form of this command. Subinterfaces require a VLAN ID to pass traffic. VLAN subinterfaces let you configure multiple logical interfaces on a single physical interface. VLANs let you keep traffic separate on a given physical interface, for example, for multiple security contexts.

> **vlan** *id*

> **no vlan**

Syntax Description	*id* Specifies an integer between 1 and 4094. Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information.

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**
Interface configuration	•	•	•	—	•

Command History

Release	Modification
7.0(1)	This command was moved from a keyword of the **interface** command to an interface configuration mode command.

Usage Guidelines   You can only assign a single VLAN to a subinterface, and not to the physical interface. Each subinterface must have a VLAN ID before it can pass traffic. To change a VLAN ID, you do not need to remove the old VLAN ID with the **no** option; you can enter the **vlan** command with a different VLAN ID, and the security appliance changes the old ID.

You need to enable the physical interface with the **no shutdown** command to let subinterfaces be enabled. If you enable subinterfaces, you typically do not also want the physical interface to pass traffic, because the physical interface passes untagged packets. Therefore, you cannot prevent traffic from passing through the physical interface by bringing down the interface. Instead, ensure that the physical interface does not pass traffic by leaving out the **nameif** command. If you want to let the physical interface pass untagged packets, you can configure the **nameif** command as usual.

The maximum number of subinterfaces varies depending on your platform. See the *Cisco Security Appliance Command Line Configuration Guide* for the maximum subinterfaces per platform.

Examples   The following example assigns VLAN 101 to a subinterface:

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example changes the VLAN to 102:

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
interface	Configures an interface and enters interface configuration mode.
show running-config interface	Shows the current configuration of the interface.

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
7.0(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** version of this command. To remove all configured Vpn address assignment methods from the security appliance, user the **no** version 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
7.0(1)(1)	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 security appliance 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 ACL to use for VPN connections, use the **vpn-filter** command in group policy or username mode. To remove the ACL, 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 ACLs to permit or deny various types of traffic for this user or group policy. You then use the **vpn-filter** command to apply those ACLs.

> **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:

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

Command History

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

Usage Guidelines   WebVPN does not use the ACL 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, or uses a downloadable 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
7.0(1)(1)	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:

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

Command History

Release	Modification
7.0(1)(1)	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
```

Note   If RADIUS only returns the subnet mask, the authentication uses the IP address from the local pool which has its own subnet netmask. It does not use the mask from RADIUS. To prevent this, return both the netmask and IP address from RADIUS.

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	•	—	•	—	—

Command History

Release	Modification
7.0(1)(1)	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 security appliance 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 security appliance 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 security appliance 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
7.0(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 security appliance terminates the connection.

vpn load-balancing

To enter vpn load-balancing mode, in which you can configure VPN load balancing and related functions, use the **vpn load-balancing** command in global configuration mode.

vpn load-balancing

✎
Note Only ASA Models 5520 and higher support VPN load balancing. VPN load balancing also requires an active 3DES/AES license. The security appliance checks for the existence of this crypto license before enabling load balancing. If it does not detect an active 3DES or AES license, the security appliance prevents the enabling of load balancing and also prevents internal configuration of 3DES by the load balancing system unless the license permits this usage.

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines Use the **vpn load-balancing** command to enter vpn load-balancing mode. The following commands are available in vpn load-balancing mode:

cluster encryption

cluster ip address

cluster key

cluster port

interface

nat

participate

priority

See the individual command descriptions for detailed information.

Examples   The following is an example of the **vpn load-balancing** command; note the change in the prompt:

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

The following is an example of a VPN load-balancing command sequence that includes an interface command that specifies the public interface of the cluster as "test" and the private interface of the cluster as "foo":

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

Command	Description
clear configure vpn load-balancing	Removes the load-balancing runtime configuration and disables load balancing.
show running-config vpn load-balancing	Displays the the current VPN load-balancing virtual cluster configuration.
show vpn load-balancing	Displays VPN load-balancing runtime statistics.

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** | **webvpn** | **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 hat 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.
webvpn	Logs off all WebVPN sessions.

Defaults

No default behavior or values.

Command Modes

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

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

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

Examples

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

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

The next 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 security appliance allows, use the **vpn-sessiondb max-session-limit** command in global configuration mode. To remove the session limit, use the **no** version 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
7.0(1)	This command was introduced.

Usage Guidelines   This command applies to IPSec VPN sessions,.

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

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

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-webvpn-session-limit	Sets a maximum number of WebVPN sessions.

vpn-sessiondb max-webvpn-session-limit

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

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

> **no vpn-sessiondb max-webvpn-session-limit**

Syntax Description	*session-limit*	Specifies the maximum number of WebVPN 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
7.1(1)	This command was introduced.

Usage Guidelines   This command applies to WebVPN sessions.

Examples   The following example shows how to set a maximum WebVPN session limit of 75:

```
hostname (config)# vpn-sessiondb max-webvpn-session-limit 75
```

Related Commands

Command	Description
vpn-sessiondb logoff	Logs off all or specific types of IPsec VPN and WebVPN sessions.
vpn-sessiondb max-vpn-session-limit	Sets a maximum number of VPN sessions.

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 security appliance 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
7.0(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 security appliance 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
7.0(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 or WebVPN), 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 {webvpn | IPSec}

no vpn-tunnel-protocol [webvpn | 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
7.0(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 WebVPN and IPSec tunneling modes for the group policy named "FirstGroup":

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

web-agent-url

To specify the SSO server URL to which the security appliance makes SSO authentication requests, use the **web-agent-url** command in webvpn-sso-siteminder configuration mode. This is an SSO with CA SiteMinder command.

To remove an SSO server authentication URL, use the **no** form of this command.

> **web-agent-url** *url*

> **no web-agent-url** *url*

Note   This command is required for SSO authentication.

Syntax Description

url	Specifies the authentication URL of the SSO server. Must contain http:// or https://.

Defaults   By default, an authentication URL is not configured.

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Webvpn-sso-siteminder configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines   Single-sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once. The SSO server has a URL that handles authentication requests.

Use the **web-agent-url** command to configure the security appliance to send authentications to this URL. Before configuring the authentication URL, you must create the SSO server using the **sso-server** command.

Examples   The following example, entered in webvpn-sso-siteminder configuration mode, specifies an authentication URL of http://www.example.com/webvpn:

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
```

```
hostname(config-webvpn-sso-siteminder)#
```

Related Commands

Command	Description
max-retry-attempts	Configures the number of times the security appliance retries a failed SSO authentication attempt.
policy-server-secret	Creates a secret key used to encrypt authentication requests to an SSO server.
request-timeout	Specifies the number of seconds before a failed SSO authentication attempt times out.
show webvpn sso-server	Displays the operating statistics for an SSO server.
sso-server	Creates a single sign-on server.

web-applications

To customize the Web Application box of the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-applications** command from webvpn customization mode:

> **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

> [**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

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

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message displayed under the title.
dropdown	Specifies you are changing the dropdown box.
text	Specifies you are changing the text.
style	Specifies you are changing the HTML style.
value	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title text is "Web Application".

The default title style is background-color:#99CCCC;color:black;font-weight:bold;text-transform: uppercase

The default message text is "Enter Web Address (URL)".

The default message style is background-color:#99CCCC;color:maroon;font-size:smaller.

The default dropdown text is "Web Bookmarks".

The default dropdown style is border:1px solid black;font-weight:bold;color:black;font-size:80%.

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 customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

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

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

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

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

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

Examples   The following example changes the title to "Applications", and the color of the text to blue:

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-applications title text Applications
F1-asa1(config-webvpn-custom)# web-applications title style color:blue
```

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-bookmarks	Customizes the Web Bookmarks title or links on the WebVPN Home page.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.

web-bookmarks

To customize the Web Bookmarks title or links on the WebVPN Home page that is displayed to authenticated WebVPN users, use the **web-bookmarks** command from webvpn customization mode:

> **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

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

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

Syntax Description

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

Defaults

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

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

The default title text is "Web Bookmarks".

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

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

- RGB format is 0,0,0, a range of decimal numbers from 0 to 255 for each color (red, green, blue); the comma separated entry indicates the level of intensity of each color to combine with the others.

- HTML format is #000000, six digits in hexadecimal format; the first and second represent red, the third and fourth green, and the fifth and sixth represent blue.

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

Examples   The following example customizes the Web Bookmarks title to "Corporate Web Bookmarks":

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-bookmarks title text Corporate Web 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.
file-bookmarks	Customizes the File Bookmarks title or links on the WebVPN Home page.
web-applications	Customizes the Web Application box of the WebVPN Home page.

webvpn (group-policy and username modes)

To enter this webvpn mode, use the **webvpn** command in group-policy configuration mode or in username configuration mode. To remove all commands entered in webvpn mode, use the **no** form of this command. These webvpn commands apply to the username or group policy from which you configure them.

Webvpn commands for group policies and usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter.

webvpn

no webvpn

Syntax Description   This command has no arguments or keywords.

Defaults   WebVPN is disabled by default.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines   Webvpn mode, which you enter from global configuration mode, lets you configure global settings for WebVPN. The **webvpn** command in group-policy attributes configuration mode or username attributes configuration mode applies the settings specified in the webvpn command to the group or user specified in the parent command. In other words, webvpn mode, described in this section, and which you enter from group-policy or username mode, lets you customize a WebVPN configuration for specific users or group policies.

The webvpn attributes that you apply for a specific group policy in group-policy attributes mode override those specified in the default group policy. The WebVPN attributes that you apply for a specific user in username attributes mode override both those in the default group policy and those in the group policy to which that user belongs. Essentially, these commands let you tweak the settings that would otherwise be inherited from the default group or the specified group policy. For information about the WebVPN settings, see the description of the **webvpn** command in global configuration mode.

The following table lists the attributes you can configure in webvpn group-policy attributes and username attributes mode. See the individual command descriptions for details.

Attribute	Description
auto-signon	Configures the security appliance to automatically pass WebVPN user login credentials on to internal servers, providing a single sign-on method for WebVPN users.
customization	Specifies a preconfigured WebVPN customization to apply.
deny-message	Specifies a message to display to the user when access is denied.
filter	Identifies the access list to be used for WebVPN connections.
functions	Configures file access and file browsing, MAPI Proxy, and URL entry over WebVPN.
homepage	Sets the URL of the webpage that displays when WebVPN users log in.
html-content-filter	Identifies Java, ActiveX, images, scripts, and cookies to filter for WebVPN sessions.
http-comp	Specifies the HTTP compression algorithm to use.
keep-alive-ignore	Specifies the maximum object size to ignore for updating the session.
port-forward	Enables WebVPN application access.
port-forward-name	Configures the display name that identifies TCP port forwarding to end users.
sso-server	Configures the SSO server name.
svc	Configures SSL VPN Client attributes.
url-list	Identifies a list of servers and URLs that users can access via WebVPN.

Examples   The following example shows how to enter webvpn mode for the group policy named "FirstGroup":

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

The following example shows how to enter webvpn mode for the username named "test":

```
hostname(config)# group-policy test attributes
hostname(config-username)# webvpn
hostname(config-webvpn)#
```

Related Commands

clear configure group-policy	Removes the configuration for a particular group policy or for all group policies.
group-policy attributes	Enters config-group-policy mode, which lets you configure attributes and values for a specified group policy or lets you enter webvpn mode to configure webvpn attributes for the group.

show running-config group-policy	Displays the running configuration for a particular group policy or for all group policies.
webvpn	Enters config-group-webvpn mode, in which you can configure the WebVPN attributes for the specified group.

who

To display active Telnet administration sessions on the security appliance, 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
Preexisting	This command was preexisting.

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 security appliance.

Examples   This example shows the output of the **who** command when a client is logged into the security appliance 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 security appliance console and sets the idle timeout.

window-variation

To drop a connection with a window size variation, use the **window-variation** command in tcp-map configuration mode. To remove this specification, use the **no** form of this command.

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

Syntax Description

allow-connection	Allows the connection.
drop-connection	Drops the connection.

Defaults   The default action is to allow the connection.

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

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

Use the **tcp-map** command to enter tcp-map configuration mode. Use the **window-variation** command in tcp-map configuration mode to drop all connections with a window size that has been shrunk.

The window size mechanism allows TCP to advertise a large window and to subsequently advertise a much smaller window without having accepted too much data. From the TCP specification, "shrinking the window" is strongly discouraged. When this condition is detected, the connection can be dropped.

Examples   The following example shows how to drop all connections with a varied window size:

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# window-variation drop-connection
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
```

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

Related Commands

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

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
7.0(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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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**

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
Preexisting	This command was preexisting.

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. 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, 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. Context startup configurations can reside on external servers. In this case, the security appliance 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. 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**

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 security appliance 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
Preexisting	This command was preexisting.

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 security appliance 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
Preexisting	This command was preexisting.

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 security appliance 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.

When Stateful Failover is enabled, the **write standby** command also replicates state information to the standby unit after the configuration replication is complete.

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
Preexisting	This command was preexisting.

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.