C H A P T E R

8

client-access-rule through crl-configure Commands

client-access-rule

To configure rules that limit the remote access client types and versions that can connect via IPSec through the FWSM, use the **client-access-rule** command in group-policy configuration mode. To delete a rule, use the **no** form of this command.

client-access-rule *priority* {**permit** | **deny**} **type** *type* **version** *version* | **none**

no client-access-rule *priority* [{**permit** | **deny**} **type** *type* **version** *version*]

Syntax Description

deny	Denies connections for devices of a particular type and/or version.
none	Allows no client access rules. Sets client-access-rule to a null value, thereby allowing no restriction. Prevents inheriting a value from a default or specified group policy.
permit	Permits connections for devices of a particular type and/or version.
priority	Determines the priority of the rule. The rule with the lowest integer has the highest priority. Therefore, the rule with the lowest integer that matches a client type and/or version is the rule that applies. If a lower priority rule contradicts, the FWSM ignores it.
type *type*	Identifies device types via free-form strings, for example VPN 3002. A string must match exactly its appearance in the **show vpn-sessiondb remote** display, except that you can use the * character as a wildcard.
version *version*	Identifies the device version via free-form strings. A string must match exactly its appearance in the **show vpn-sessiondb remote** display, except that you can use the * character as a wildcard.

Defaults

By default, there are no access rules.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

To delete all rules, use the **no client-access-rule command** with only the priority argument. This deletes all configured rules, including a null rule created by issuing the **client-access-rule none** command.

When there are no client access rules, users inherit any rules that exist in the default group policy. To prevent users from inheriting client access rules, use the **client-access-rule none** command. The result of doing so is that all client types and versions can connect.

Construct rules according to these caveats:

- If you do not define any rules, the FWSM permits all connection types.

- When a client matches none of the rules, the FWSM denies the connection. This means that if you define a deny rule, you must also define at least one permit rule, or the FWSM denies all connections.

- For both software and hardware clients, type and version must match exactly their appearance in the **show vpn-sessiondb remote** display.

- The * character is a wildcard, which you can use multiple times in each rule. For example, **client-access-rul**e **3 deny type * version 3.*** creates a priority 3 client access rule that denies all client types running software Version 3.x software.

- You can construct a maximum of 25 rules per group policy.

- There is a limit of 255 characters for an entire set of rules.

- You can use n/a for clients that do not send client type and/or version.

Examples
The following example shows how to create client access rules for the group policy named FirstGroup. These rules permit VPN clients running software Version 4.1, while denying all VPN 3002 hardware clients:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-firewall

To set personal firewall policies that the FWSM pushes to the VPN client during IKE tunnel negotiation, use the **client-firewall** command in group-policy configuration mode. To delete a firewall policy, use the **no** form of this command.

> **client-firewall none**
>
> **client-firewall opt | req custom vendor-id** *num* **product-id** *num* **policy AYT | {CPP acl-in** *ACL* **acl-out** *ACL*} [**description** *string*]
>
> **client-firewall opt | req zonelabs-zonealarm policy AYT | {CPP acl-in** *ACL* **acl-out** *ACL*}
>
> **client-firewall opt | req zonelabs-zonealarmorpro policy AYT | {CPP acl-in** *ACL* **acl-out** *ACL*}
>
> **client-firewall opt | req zonelabs-zonealarmpro policy AYT | {CPP acl-in** *ACL* **acl-out** *ACL*}
>
> **client-firewall opt | req cisco-integrated acl-in** *ACL* **acl-out** *ACL*
>
> **client-firewall opt | req sygate-personal**
>
> **client-firewall opt | req sygate-personal-pro**
>
> **client-firewall opt | req sygate-security-agent**
>
> **client-firewall opt | req networkice-blackice**
>
> **client-firewall opt | req cisco-security-agent**

Syntax Description		
acl-in *<ACL>*	Provides the policy the client uses for inbound traffic.
acl-out *<ACL>*	Provides the policy the client uses for outbound traffic.
AYT	Specifies that the client PC firewall application controls the firewall policy. The FWSM checks to make sure the firewall is running. It asks, "Are You There?" If there is no response, the FWSM tears down the tunnel.
cisco-integrated	Specifies Cisco Integrated firewall type.
cisco-security-agent	Specifies Cisco Intrusion Prevention Security Agent firewall type.
CPP	Specifies Policy Pushed as source of the VPN client firewall policy.
custom	Specifies Custom firewall type.
description *<string>*	Describes the firewall.
networkice-blackice	Specifies Network ICE Black ICE firewall type.
none	Indicates that there is no client firewall policy. Sets a firewall policy with a null value, thereby disallowing one. Prevents inheriting a firewall policy from a default or specified group policy.
opt	Indicates an optional firewall type.
product-id	Identifies the firewall product.
req	Indicates a required firewall type.
sygate-personal	Specifies Sygate Personal firewall type.
sygate-personal-pro	Specifies Sygate Personal Pro firewall type.

sygate-security-agent	Specifies Sygate Security Agent firewall type.
vendor-id	Identifies the firewall vendor.
zonelabs-zonealarm	Specifies Zone Labs Zone Alarm firewall type.
zonelabs-zonealarmorpro policy	Specifies Zone Labs Zone Alarm or Pro firewall type.
zonelabs-zonealarmpro policy	Specifies Zone Labs Zone Alarm Pro firewall type.

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 configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines   Only one instance of this command can be configured.

To delete all firewall policies, use the **no client-firewall** command without arguments. This deletes all configured firewall policies, including a null policy created by issuing the **client-firewall none** command.

When there are no firewall policies, users inherit any that exist in the default or other group policy. To prevent users from inheriting such firewall policies, use the **client-firewall none** command.

Examples   The following example shows how to set a client firewall policy that requires Cisco Intrusion Prevention Security Agent for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client-update

To configure and change client update parameters, use the **client-update** command in tunnel-group ipsec-attributes configuration mode. To disable a client update, use the **no** form of this command.

client-update type *type* {**url** *url-string*} {**rev-nums** *rev-nums*}

no client-update [*type*]

Syntax Description

rev-nums *rev-nums*	Specifies the software or firmware images for this client. Enter up to 4, separated by commas.
type	Specifies the operating systems to notify of a client update. The list of operating systems comprises the following: • Windows: all windows-based platforms • WIN9X: Windows 95, Windows 98, and Windows ME platforms • WinNT: Windows NT 4.0, Windows 2000, and Windows XP platforms • vpn3002: VPN 3002 hardware client
url *url-string*	Specifies the URL for the software/firmware image. This URL must point to a file appropriate for this client.

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**
Tunnel-group ipsec-attributes configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines   If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update. You can specify up to 4 of these client update entries.

You can apply this attribute to IPSec remote-access tunnel-group type only. If the client is already running a software version on the list of revision numbers, it does not need to update its software. If the client is not running a software version on the list, it should update.

Examples   The following example entered in config-ipsec configuration mode, configures client update parameters for the remote-access tunnel-group remotegrp. It designates the revision number, 4.6.1 and the URL for retrieving the update, which is https://support/updates.

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-ipsec)# client-update type windows url https://support/updates/ rev-nums
4.6.1
hostname(config-ipsec)#
```

Related Commands

Command	Description
clear configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the indicated certificate map entry.
tunnel-group-map enable	Associates the certificate map entries created using the **crypto ca certificate map** command with tunnel groups.

command-alias

To create an alias for a command, use the **command-alias** command in global configuration mode. To remove the alias, use the **no** form of this command.

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

Syntax Description

command_alias	Specifies the new name you want for an existing command.
mode	Specifies the command mode in which you want to create the command alias, for example **exec** (for user and privileged EXEC modes), **configure**, or **interface**.
original_command	Specifies the existing command or command with its keywords for which you want to create the command alias.

Defaults

By default, the following user EXEC mode aliases are configured:

h for **help**

lo for **logout**

p for **ping**

s for **show**

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

When you enter the command alias, the original command is invoked. You might want to create command aliases to provide shortcuts for long commands, for example.

You can create an alias for the first part of any command and still enter the additional keywords and arguments as normal.

When you use CLI help, command aliases are indicated by an asterisk (*), and displayed in the following format:

```
*command-alias=original-command
```

For example, the **lo** command alias displays along with other privileged EXEC mode commands that start with "lo," as follows:

```
hostname# lo?
*lo=logout login  logout
```

You can use the same alias in different modes. For example, you can use "happy" in privileged EXEC mode and configuration mode to alias different commands, as follows:

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

To list only commands and omit aliases, begin your input line with a space. Also, to circumvent command aliases, use a space before entering the command. In the following example, the alias happy is not shown, because there is a space before the happy? command.

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#    happy?
ERROR: % Unrecognized command
```

As with commands, you can use CLI help to display the arguments and keywords that can follow a command alias.

You must enter the complete command alias. Shortened aliases are not accepted. In the following example, the parser does not recognize the command hap as indicating the alias happy:

```
hostname# hap
% Ambiguous command: "hap"
```

Examples   The following example shows how to create a command alias named "**save**" for the **copy running-config startup-config** command:

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

Related Commands

Command	Description
clear configure command-alias	Clears all non-default command aliases.
show running-config command-alias	Displays all non-default command aliases configured.

command-queue

To specify the maximum number of MGCP commands that are queued while waiting for a response, use the **command-queue** command in mgcp map configuration mode. To remove the configuration, use the **no** form of this command.

command-queue *limit*

no command-queue *limit*

Syntax Description

limit	Specifies the maximum number of commands to queue, from 1 to 2147483647.

Defaults

This command is disabled by default.

The default for the MGCP command queue is 200.

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
Mgcp map configuration	•	•	•	•	—

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

Use the **command-queue** command to specify the maximum number of MGCP commands that are queued while waiting for a response. The range of allowed values is from 1 to 4294967295. The default is 200. When the limit has been reached and a new command arrives, the command that has been in the queue for the longest time is removed.

Examples

The following example limits the MGCP command queue to 150 commands:

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

Related Commands

Commands	Description
debug mgcp	Enables the display of debug information for MGCP.
mgcp-map	Defines an MGCP map and enables MGCP map configuration mode.
show mgcp	Displays MGCP configuration and session information.

Commands	Description
timeout [**mgcp**]	Configures the idle timeout after which an MGCP media connection will be closed.
timeout [**mgcp-pat**]	Configures the idle timeout after which an MGCP PAT xlate will be removed.

compatible rfc1583

To restore the method that is used to calculate the summary route costs per RFC 1583, use the **compatible rfc1583** command in router configuration mode. To disable RFC 1583 compatibility, use the **no** form of this command.

>   **compatible rfc1583**

>   **no compatible rfc1583**

Syntax Description   This command has no arguments or keywords.

Defaults   This command is enabled 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
Router configuration	●	—	●	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines   Only the **no** form of this command appears in the configuration.

Examples   The following example shows how to disable RFC 1583-compatible route summary cost calculation:

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

Related Commands

Command	Description
router ospf	Enters router configuration mode.
show running-config router	Displays the commands in the global router configuration.

configure http

To merge a configuration file from an HTTP(S) server with the running configuration, use the **configure http** command in global configuration mode. This command supports IPv4 and IPv6 addresses.

configure http[**s**]**://**[*user*[**:**password]**@**]*server*[*:port*]/[*path/*]*filename*

Syntax Description

:password	(Optional) For HTTP(S) authentication, specifies the password.
:port	(Optional) Specifies the port. For HTTP, the default is 80. For HTTPS, the default is 443.
@	(Optional) If you enter a name and/or a password, precedes the server IP address with an at sign (@).
filename	Specifies the configuration filename.
http[**s**]	Specifies either HTTP or HTTPS.
path	(Optional) Specifies a path to the filename.
server	Specifies the server IP address or name. For IPv6 server addresses, if you specify the port, then you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the port number. For example, enter the following address and port: `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	(Optional) For HTTP(S) authentication, specifies the username.

Defaults

For HTTP, the default port is 80. For HTTPS, the default port is 443.

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
2.2(1)	This command was introduced.

Usage Guidelines

A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

This command is the same as the **copy http running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure http** command is an alternative for use within a context.

Examples   The following example copies a configuration file from an HTTPS server to the running configuration:

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

Related Commands

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

configure memory

To merge the startup configuration with the running configuration, use the **configure memory** command in global configuration mode.

> **configure 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines   A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the FWSM, and then enter the **configure memory** command to load the new configuration.

This command is equivalent to the **copy startup-config running-config** command.

For multiple context mode, a context startup configuration is at the location specified by the **config-url** command.

Examples   The following example copies the startup configuration to the running configuration:

```
hostname(config)# configure memory
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
configure factory-default	Adds commands you enter at the CLI to the running configuration.
show running-config	Shows the running configuration.

configure net

To merge a configuration file from a TFTP server with the running configuration, use the **configure net** command in global configuration mode. This command supports IPv4 and IPv6 addresses.

> **configure net** [*server***:**[*filename*] | **:***filename*]

Syntax Description

:*filename*	Specifies the path and filename. If you already set the filename using the **tftp-server** command, then this argument is optional.
	If you specify the filename in this command as well as a name in the **tftp-server** command, the FWSM treats the **tftp-server** command filename as a directory, and adds the **configure 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 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. For IPv6 server addresses, you must enclose the IP address in brackets so that the colons in the IP address are not mistaken for the colon before the filename. For example, enter the following address:
	[fe80::2e0:b6ff:fe01:3b7a]
	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**
Global configuration	•	•	•	•	•

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines   A merge adds all commands from the new configuration to the running configuration, and overwrites any conflicting commands with the new versions. For example, if a command allows multiple instances, the new commands are added to the existing commands in the running configuration. If a command allows only one instance, the new command overwrites the command in the running configuration. A merge never removes commands that exist in the running configuration but are not set in the new configuration.

This command is the same as the **copy tftp running-config** command. For multiple context mode, that command is only available in the system execution space, so the **configure net** command is an alternative for use within a context.

Examples   The following example sets the server and filename in the **tftp-server** command, and then overrides the server using the **configure net** command. The same filename is used.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

The following example overrides the server and the filename. The default path to the filename is /tftpboot/configs/config1. The /tftpboot/ part of the path is included by default when you do not lead the filename with a slash (/). Because you want to override this path, and the file is also in tftpboot, include the tftpboot path in the **configure net** command.

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

Related Commands

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

configure terminal

To configure the running configuration at the command line, use the **configure terminal** command in privileged EXEC mode. This command enters global configuration mode, which lets you enter commands that change the configuration.

configure 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:

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

Command History

Release	Modification
2.2(1)	This command was introduced.

Examples   The following example enters global configuration mode:

```
hostname# configure terminal
hostname(config)#
```

Related Commands

Command	Description
clear configure	Clears the running configuration.
configure http	Merges a configuration file from the specified HTTP(S) URL with the running configuration.
configure memory	Merges the startup configuration with the running configuration.
configure net	Merges a configuration file from the specified TFTP URL with the running configuration.
show running-config	Shows the running configuration.

config-url

To identify the URL from which the system downloads the context configuration mode, use the **config-url** command in context configuration mode.

config-url *url*

Syntax Description	*url* Sets the context configuration URL. All remote URLs must be accessible from the admin context. See the following URL syntax:

- **disk:/**[*path/*]*filename*

    This URL indicates the internal Flash memory.

- **ftp://**[*user*[**:**password]**@**]*server*[:*port*]**/**[*path/*]*filename*[**;type=**xx]

    The FTP path on the server is a relative path (*path/filename*). To use an absolute path (*/path/filename*), enter an extra slash (/) after the server address:

    ftp://server**//**[*path/*]*filename*

    The **type** can be one of the following keywords:

    - **ap**—ASCII passive mode
    - **an**—ASCII normal mode
    - **ip**—(Default) Binary passive mode
    - **in**—Binary normal mode

- **http**[**s**]**://**[*user*[**:**password]**@**]*server*[:*port*]**/**[*path/*]*filename*

- **tftp://**[*user*[**:**password]**@**]*server*[:*port*]**/**[*path/*]*filename*[**;int=**interface_name]

    Specify the interface name if you want to override the route to the 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**
Context configuration	N/A	N/A	—	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines   When you add a context URL, the system immediately loads the context so that it is running.

> **Note**   Enter the **allocate-interface** command(s) before you enter the **config-url** command. The FWSM must assign interfaces to the context before it loads the context configuration; the context configuration might include commands that refer to interfaces (**interface**, **nat**, **global**...). If you enter the **config-url** command first, the FWSM loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

The filename does not require a file extension, although we recommend using ".cfg".

The admin context file must be stored on the internal Flash memory.

If you download a context configuration from an HTTP or HTTPS server, you cannot save changes back to these servers using the **copy running-config startup-config** command. You can, however, use the **copy tftp** command to copy the running configuration to a TFTP server.

If the system cannot retrieve the context configuration file because the server is unavailable, or the file does not yet exist, the system creates a blank context that is ready for you to configure with the command-line interface.

To change the URL, reenter the **config-url** command with a new URL. The FWSM merges the new configuration with the current running configuration. Reentering the same URL also merges the saved configuration with the running configuration. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results. If the running configuration is blank (for example, if the server was unavailable and the configuration was never downloaded), then the new configuration is used. If you do not want to merge the configurations, you can clear the running configuration, which disrupts any communications through the context, and then reload the configuration from the new URL.

Examples   The following example sets the admin context to be "administrator," creates a context called "administrator" on the internal Flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# class gold
hostname(config-ctx)# allocate-acl-partition 0


hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# class silver
```

Related Commands	Command	Description
	allocate-interface	Allocates interfaces to a context.
	context	Creates a security context in the system configuration and enters context configuration mode.
	show context	Shows a list of contexts (system execution space) or information about the current context.

console timeout

To set the idle timeout for a console connection to the FWSM, use the **console timeout** command in global configuration mode. To disable, use the **no** form of this command.

> **console timeout** *number*

> **no console timeout** [*number*]

Syntax Description

| *number* | Specifies the idle time in minutes (0 through 60) after which the console session ends. |

Defaults

The default timeout is 0, which means the console session will not time out.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The **console timeout** command does not alter the Telnet or SSH timeouts; these access methods maintain their own timeout values using the **timeout** command.

The **no console timeout** command resets the console timeout value to the default timeout of 0, which means that the console will not time out.

Examples

The following example shows how to set the console timeout to 15 minutes:

```
hostname(config)# console timeout 15
```

Related Commands

Command	Description
clear configure console	Restores the default console connection settings.
show running-config console timeout	Displays the idle timeout for a console connection to the FWSM.
timeout	Sets the idle time for connection, translation UDP, and RPC slots.

content-length

To restrict HTTP traffic based on the length of the HTTP message body, use the **content-length** command in HTTP map configuration mode, which is accessible using the **http-map** command. To remove this command, use the **no** form of this command.

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description		
	action	Specifies the action taken when a message fails this inspection.
	allow	Allows the message.
	bytes	Specifies the number of bytes. The permitted range is 1 to 65535 for the **min** option and 1 to 50000000 for the **max** option.
	drop	Closes the connection.
	log	(Optional) Generates a syslog.
	max	(Optional) Specifies the maximum content length allowed.
	min	Specifies the minimum content length allowed.
	reset	Sends a TCP reset message to client and server.

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
Http map configuration	•	•	•	•	—

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines After enabling the **content-length** command, the FWSM only allows messages within the configured range and otherwise takes the specified action. Use the **action** keyword to cause the FWSM to reset the TCP connection and create a syslog entry.

Examples   The following example restricts HTTP traffic to messages 100 bytes or larger and not exceeding 2000 bytes. If a message is outside this range, the FWSM resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

content-type-verification

To restrict HTTP traffic based on the content type of the HTTP message, use the **content-type-verification** command, in HTTP map configuration mode, which is accessible using the **http-map** command. To disable this feature, use the **no** form of the command.

content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

no content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

Syntax Description

action	Specifies the action taken when a message fails command inspection.
allow	Allows the message.
drop	Closes the connection.
log	(Optional) Generates a syslog message.
match-req-rsp	(Optional) Verifies that the content-type field in the HTTP response matches the accept field in the corresponding HTTP request message.
reset	Sends a TCP reset message to client and server.

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**
Http map configuration	•	•	•	•	—

Command History

Release	Modification
3.1	This command was introduced

Usage Guidelines   This command enables the following checks:

- Verifies that the value of the header content-type is in the internal list of supported content types,

- Verifies that the header content-type matches the actual content in the data or entity body portion of the message.

- The **match-req-rsp** keyword enables an additional check that verifies the content-type field in the HTTP response matches the **accept** field in the corresponding HTTP request message.

If the message fails any of the above checks, the FWSM takes the configured action.

The following table lists the supported content types.

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

Some content-types in this list may not have a corresponding regular expression (magic number) so they cannot be verified in the body portion of the message. When this case occurs, the HTTP message will be allowed.

Examples   The following example restricts HTTP traffic based on the content type of the HTTP message. If a message contains an unsupported content type, the FWSM resets the TCP connection and creates a syslog entry.

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# exit
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
http-map	Defines an HTTP map for configuring enhanced HTTP inspection.
debug appfw	Displays detailed information about traffic associated with enhanced HTTP inspection.
inspect http	Applies a specific HTTP map to use for application inspection.
policy-map	Associates a class map with specific security actions.

context

To create a security context in the system configuration and enter context configuration mode, use the **context** command in global configuration mode. To remove a context, use the **no** form of this command. In context configuration mode, you can identify the configuration file URL and interfaces that a context can use.

context *name*

no context *name* [**noconfirm**]

Syntax Description		
name	Sets the name as a string up to 32 characters long. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen.	
	"System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.	
noconfirm	(Optional) Removes the context without prompting you for confirmation. This option is useful for automated scripts.	

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	N/A	N/A	—	—	•

Command History	Release	Modification
	2.2(1)	This command was introduced.

Usage Guidelines   If you do not have an admin context (for example, if you clear the configuration) then the first context you add must be the admin context. To add an admin context, see the **admin-context** command. After you specify the admin context, you can enter the **context** command to configure the admin context.

You can only remove a context by editing the system configuration. You cannot remove the current admin context using the **no** form of this command; you can only remove it if you remove all contexts using the **clear configure context** command.

Examples   The following example sets the admin context to be "administrator," creates a context called "administrator" on the internal Flash memory, and then adds two contexts from an FTP server:

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface vlan10
hostname(config-ctx)# allocate-interface vlan11
hostname(config-ctx)# config-url disk:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface vlan100 int1
hostname(config-ctx)# allocate-interface vlan102 int2
hostname(config-ctx)# allocate-interface vlan110-vlan115 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
hostname(config-ctx)# allocate-acl-partition 0

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface vlan200 int1
hostname(config-ctx)# allocate-interface vlan212 int2
hostname(config-ctx)# allocate-interface vlan230-vlan235 int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
hostname(config-ctx)# member silver
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces to a context.
changeto	Changes between contexts and the system execution space.
config-url	Specifies the location of the context configuration.
join-failover-group	Assigns a context to a failover group.
show context	Shows context information.

control-point tcp-normalizer

To enable the TCP normalizing function, use the **control-point tcp-normalizer** command in global configuration mode. To disable the TCP normalizer, use the **no** form of this command.

control-point tcp-normalizer

no control-point tcp-normalizer

Syntax Description   This command has no arguments or keywords.

Defaults   The TCP normalizer is enabled by default.

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

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

Command History

Release	Modification
3.1(4)	This command was introduced.

Usage Guidelines   The TCP normalizer feature performs a set of extra actions on certain TCP traffic flows that pass through the FWSM. Specifically, only traffic that passes through the control-plane path is subject to the actions of the TCP normalizer. Traffic that passes through the accelerated path (such as TCP or UDP traffic that is not subject to application inspection by the FWSM) is never subject to the TCP normalizer. The TCP normalizer is enabled by default, and is not configurable except to enable or disable it.

The following additional security checks are performed by the TCP normalizer:

- The TTL value of IP packets in a flow is verified.

- If packets in a flow are out of order, the FWSM attempts to re-order the packets.

- TCP state and windowing checks.

- TCP PAWS checks.

- Additional atomic TCP checks.

You might want to disable the TCP normalizer for testing purposes.

When you disable the TCP normalizer, new flows do not use the TCP normalizer, but existing flows continue to use the TCP normalizer.

Examples   The following example disables the TCP normalizer:

```
hostname(config)# no control-point tcp-normlaizer
```

Related Commands	Command	Description
	set connection	Sets connection limits.

copy

To copy a file from one location to another, use the **copy** command in privileged EXEC mode.

copy [**/noconfirm**] {*url* | **running-config** | **startup-config**} {**running-config** | **startup-config** | *url*}

Syntax Description		
/noconfirm	Copies the file without a confirmation prompt.
running-config	Specifies the running configuration.
startup-config	Specifies the startup configuration. The startup configuration for single mode or for the system in multiple context mode is a hidden file in flash memory. From within a context, the location of the startup configuration is specified by the **config-url** command. For example, if you specify an HTTP server for the **config-url** command and then enter the **copy startup-config running-config** command, the FWSM copies the startup configuration from the HTTP server using the admin context interface.

url	Specifies the source or destination file to be copied. Not all combinations of source and destination URLs are allowed. For example, you cannot copy from a remote server to another remote server; this command is meant to copy between local and remote locations. In a context, you can copy the running or startup configuration to a TFTP or FTP server using the context interfaces, but you cannot copy from a server to the running or startup configuration. See the **startup-config** keyword for other options. Also, see the **configure net** command to download from a TFTP server to the running context configuration.

See the following URL syntax:

- **disk:/**[*path/*]*filename*

  This option indicates the configuration partition of the internal flash memory.

- **ftp://**[*user*[**:***password*]**@**]*server*[**:***port*]**/**[*path/*]*filename*[**;type=***xx*]

  The FTP path on the server is a relative path (*path/filename*). To use an absolute path (*/path/filename*), enter an extra slash (*/*) after the server address:

  ftp://*server***//**[*path/*]*filename*

  The **type** can be one of the following keywords:

  - **ap**—ASCII passive mode
  - **an**—ASCII normal mode
  - **ip**—(Default) Binary passive mode
  - **in**—Binary normal mode

- **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*]**/**[*path/*]*filename*

- **tftp://**[*user*[**:***password*]**@**]*server*[**:***port*]**/**[*path/*]*filename*[**;int=***interface_name*]

  Specify the interface name if you want to override the route to the server address.

  The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command.

  The path after the server address is a relative path (*path/file*). To make it an absolute path (*/path/file*), use two slashes after the server, for example:

  tftp://*server***//***path/filename*

Defaults   This command has no default settings.

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

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

■ **copy**

Command History	Release	Modification
	2.2(1)	This command was introduced.
	3.1(1)	The ability to copy from a context to a server was added.

Usage Guidelines   When you copy a configuration to the running configuration, you merge the two configurations. A merge adds any new commands from the new configuration to the running configuration. If the configurations are the same, no changes occur. If commands conflict or if commands affect the running of the context, then the effect of the merge depends on the command. You might get errors, or you might have unexpected results.

Examples   The following example shows how to copy a file from the disk to a TFTP server in the system execution space:

```
hostname(config)# copy disk:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

> ✎
>
> **Note**   If the **tftp-server** command defines an interface different than the location you wish to copy the a file from, you must use the **int** keyword to override the interface specified in the **tftp-server** command, or the device will attempt to copy the file from that interface.

The following example shows how to copy a file from one location on the disk to another location on the disk. The name of the destination file can be either the name of the source file or a different name.

```
hostname(config)# copy disk:my_context.cfg disk:my_context/my_context.cfg
```

The following example shows how to copy an ASDM file from a TFTP server to the flash partition:

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin flash:asdm
```

The following example shows how to copy the running configuration in a context to a TFTP server:

```
hostname(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

Related Commands	Command	Description
	configure net	Copies a file from a TFTP server to the running configuration.
	copy capture	Copies a capture file to a TFTP server.
	tftp-server	Sets the default TFTP server.
	write memory	Saves the running configuration to the startup configuration.
	write net	Copies the running configuration to a TFTP server.

copy capture

To copy a capture file to a server, use the **copy capture** command in privileged EXEC mode.

copy [**/noconfirm**] [**/pcap**] **capture:** [*context_name*/]*buffer_name url*

Syntax Description		
	buffer_name	Specifies a unique name that identifies the capture.
	context_name/	Copies a packet capture defined in a security context.
	/noconfirm	Copies the file without a confirmation prompt.
	/pcap	Copies the packet capture as raw data.
	url	Specifies the destination to copy the packet capture file. See the following URL syntax:

url (continued):

- **disk:/**[*path*/]*filename*

  This option indicates the configuration partition of the internal Flash memory.

- **ftp://**[*user*[**:**password]**@**]*server*[**:**port]**/**[*path*/]*filename*[**;type=***xx*]

  The FTP path on the server is a relative path (*path/filename*). To use an absolute path (*/path/filename*), enter an extra slash (/) after the server address:

  ftp://*server***//**[*path*/]*filename*

  The **type** can be one of the following keywords:

  – **ap**—ASCII passive mode

  – **an**—ASCII normal mode

  – **ip**—(Default) Binary passive mode

  – **in**—Binary normal mode

- **http**[**s**]**://**[*user*[**:**password]**@**]*server*[**:**port]**/**[*path*/]*filename*

- **tftp://**[*user*[**:**password]**@**]*server*[**:**port]**/**[*path*/]*filename*[**;int=***interface_name*]

  Specify the interface name if you want to override the route to the server address.

  The pathname cannot contain spaces. If a pathname has spaces, set the path in the **tftp-server** command instead of in the **copy tftp** command.

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	
Command Mode	Routed	Transparent	Single	Context	System
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
2.2(1)	This command was introduced.

Usage Guidelines   In multiple context mode, enter this command in the system execution space; you cannot enter this command within a context.

Examples   The following example shows the prompts that are provided when you enter the **copy capture** command without specifying the full path:

```
hostname# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!!
```

The following example shows how to specify the full path:

```
hostname# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

The following example shows how the location or filename can be overridden if the TFTP server is already configured:

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

The following example shows how to copy a capture from within a context in multiple context mode. You must specify the context name:

```
hostname/Context1# capture abc access-list test interface inside
hostname/Context1# changeto system
hostname# copy capture:Context1/abc tftp:171.68.11.129/tftpboot/abc.cap
```

Related Commands

Command	Description
capture	Enables packet capture capabilities for packet sniffing and network fault isolation.
clear capture	Clears the capture buffer.
show capture	Displays the capture configuration when no options are specified.

copy optimized-running-config

To replace the original non-optimized access lists with the optimized access lists, use the **copy optimized-running-config** command in privileged EXEC mode.

copy optimized-running-config running-config

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
4.0(1)	This command was introduced.

Usage Guidelines   Having access list optimization enabled at all times could be a waste of computational and memory resources. If you are satisfied with how the optimized access lists are merged, you can replace the original access lists with the optimized ones. Note that this action will wipe out all of the original access lists. After copying the optimized access lists, you may want to disable access list optimization because the newly copied optimized access lists may not be further optimized.

✎

Note   The **copy optimized-running-config** command overwrites the running configuration, and if you save the configuration, the object-group access list lines may be lost from the running config. Since optimized configurations usually contain more regular ACEs than object-group ACEs, this operation can increase the running configuration size. With a large number of access lists in a configuration, this operation can cause large configuration files that are over 3 MB in size. Therefore, use this command when you are sure that you will not exceed the start-up configuration size limit.

Examples   The following example shows how to replace the original non-optimized access lists with the optimized ones:

```
hostname(config)# copy optimized-running-config running-config
```

Related Commands

Command	Description
access-list optimization enable	Enables access list optimization.
show running-config access-list	Displays the current running access-list configuration.
debug acl optimization	Debugs access list optimization.
write memory	Saves the running configuration to the startup configuration.

cpu threshold rising

To enable configuration of the CPU threshold, use the **cpu threshold rising** command in global configuration mode. To disable configuration, use the **no** form of this command.

[**no**] **cpu threshold rising** [*threshold_value%*] [*monitoring_interval*]

Syntax Description	**monitoring_period**	Sets the CPU usage monitoring period (60-3600 sec).
	threshold_value	Sets the CPU usage threshold value (10-100%).

Defaults

The default configuration has the CPU threshold and monitoring period disabled.

Command Modes

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

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

Command History

Release	Modification
3.2(1)	This command was introduced.

Usage Guidelines

To send CPU threshold information to the NMS, enter the **logging history** command, and enable logging using the **logging enable** command. To remove the cpu threshold configuration, use the **clear config all** or **clear config cpu** command.

Note In system mode, if the CPU threshold and monitoring interval are configured, these values are effective only when the **snmp-server enable traps cpu threshold** command is configured in Admin context.

Examples

The following example configures the CPU utilization threshold value as 75% and the monitoring period as 300 seconds.

```
hostname(config)# cpu?
configure mode commands/options:
threshold Configure CPU utilization threshold parameters
exec mode commands/options:
profile CPU profiler
hostname (config)# cpu threshold?
configure mode commands/options:
rising Configure CPU rising threshold parameters
hostname (config)# cpu threshold rising?
configure mode commands/options:
WORD CPU rising threshold value (10-100%)
hostname (config)# cpu threshold rising 75%?
configure mode commands/options:
60-3600 CPU rising threshold monitoring period (60-3600 seconds)
hostname (config)# cpu threshold rising 75% 300
```

Related Commands	Command	Description
	snmp-server enable	Enables SNMP on the FWSM.
	snmp-server enable traps	Enables SNMP traps on the FWSM.

crashinfo force

To force the FWSM to crash, use the **crashinfo force** command in privileged EXEC mode.

> **crashinfo force** [**page-fault | watchdog**]

Syntax Description

page-fault	(Optional) Forces a crash of the FWSM as a result of a page fault.
watchdog	(Optional) Forces a crash of the FWSM as a result of watchdogging.

Defaults

The FWSM saves the crash information file to Flash memory 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**
Privileged EXEC	•	•	•	—	•

Command History

Release	Modification
3.1	This command was introduced.

Usage Guidelines

You can use the **crashinfo force** command to test the crash output generation. In the crash output, there is nothing that differentiates a real crash from a crash resulting from the **crashinfo force page-fault** or **crashinfo force watchdog** command (because these are real crashes). The FWSM reloads after the crash dump is complete.

⚠

Caution   Do not use the **crashinfo force** command in a production environment. The **crashinfo force** command crashes the FWSM and forces it to reload.

Examples

The following example shows the warning that displays when you enter the **crashinfo force page-fault** command:

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
   Do you wish to proceed? [confirm]:
```

If you enter a carriage return (by pressing the Return or Enter key on your keyboard), "**Y**", or "**y**" the FWSM crashes and reloads; any of these responses are interpreted as confirmation. Any other character is interpreted as a **no**, and the FWSM returns to the command-line prompt.

Related Commands	**clear crashinfo**	Clears the contents of the crash information file.
	crashinfo save disable	Disables crash information from writing to Flash memory.
	crashinfo test	Tests the ability of the FWSM to save crash information to a file in Flash memory.
	show crashinfo	Displays the contents of the crash information file.

crashinfo save disable

To disable crash information from writing to Flash memory, use the **crashinfo save** command in global configuration mode.

crashinfo save disable

no crashinfo save disable

Syntax Description   This command has no default arguments or keywords.

Defaults   The FWSM saves the crash information file to Flash memory by default.

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

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

Command History

Release	Modification
3.1(1)	The **crashinfo save enable** command was deprecated and is no longer a valid option. Use the **no crashinfo save disable** command instead.

Usage Guidelines   Crash information writes to Flash memory first, and then to your console.

Note   If the FWSM crashes during startup, the crash information file is not saved. The FWSM must be fully initialized and running first, before it can save crash information to Flash memory.

Use the **no crashinfo save disable** command to re-enable saving the crash information to Flash memory.

Examples   hostname(config)# **crashinfo save disable**

Related Commands

clear crashinfo	Clears the contents of the crash file.
crashinfo force	Forces a crash of the FWSM.
crashinfo test	Tests the ability of the FWSM to save crash information to a file in Flash memory.
show crashinfo	Displays the contents of the crash file.

crashinfo test

To test the ability of the FWSM to save crash information to a file in Flash memory, use the **crashinfo test** command in global configuration mode.

crashinfo test

Syntax Description   This command has no arguments or keywords.

Defaults   No default behavior or values.

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines   If a previous crash information file already exists in Flash memory, that file is overwritten.

Note   Entering the **crashinfo test** command does not crash the FWSM.

Examples   The following example shows the output of a crash information file test.

```
hostname(config)# crashinfo test
```

Related Commands

clear crashinfo	Deletes the contents of the crash file.
crashinfo force	Forces the FWSM to crash.
crashinfo save disable	Disables crash information from writing to Flash memory.
show crashinfo	Displays the contents of the crash file.

crl

To specify CRL configuration options, use the **crl** command in crypto ca trustpoint configuration mode.

crl {**required** | **optional** | **nocheck**}

Syntax Description

nocheck	Directs the FWSM not to perform CRL checking.
optional	The FWSM can still accept the peer certificate if the required CRL is not available.
required	The required CRL must be available for a peer certificate to be validated.

Defaults   The default value is **nocheck**.

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples   The following example enters crypto ca trustpoint configuration mode for trustpoint central, and requires that a CRL be available for a peer certificate to be validated for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters trustpoint configuration mode.
crl configure	Enters crl configuration mode.

crl configure

To enter CRL configuration configuration mode, use the **crl configure** command in crypto ca trustpoint configuration mode.

crl configure

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
Crypto ca trustpoint configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples   The following example enters crl configuration mode within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)#
```

Related Commands

Command	Description
clear configure crypto ca trustpoint	Removes all trustpoints.
crypto ca trustpoint	Enters trustpoint configuration mode.