



CHAPTER

11

default through drop Commands

default (crl configure)

To return all CRL parameters to their system default values, use the **default** command in crl configure configuration mode. The crl configure configuration mode is accessible from the crypto ca trustpoint configuration mode. These parameters are used only when the LDAP server requires them.

default

Syntax Description This command has no arguments or keywords.

Defaults No default behaviors or values.

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

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

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines Invocations of this command do not become part of the active configuration.

Examples The following example enters ca-crl configuration mode, and returns CRL command values to their defaults:

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

Related Commands	Command	Description
	crl configure	Enters crl configure configuration mode.
	crypto ca trustpoint	Enters trustpoint configuration mode.
	protocol ldap	Specifies LDAP as a retrieval method for CRLs.

default (time-range)

To restore default settings for the **absolute** and **periodic** commands, use the **default** command in time-range configuration mode.

default { **absolute** | **periodic** *days-of-the-week time to [days-of-the-week] time* }

Syntax Description

absolute	Defines an absolute time when a time range is in effect.
days-of-the-week	The first occurrence of this argument is the starting day or day of the week that the associated time range is in effect. The second occurrence is the ending day or day of the week the associated statement is in effect. This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are: • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday If the ending days of the week are the same as the starting days of the week, you can omit them.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time	Specifies the time in the format HH:MM. For example, 8:00 is 8:00 a.m. and 20:00 is 8:00 p.m.
to	Entry of the to keyword is required to complete the range “from start-time to end-time.”

Defaults

There are no default settings for this command.

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
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

If the end days-of-the-week value is the same as the start value, you can omit them.

If a **time-range** command has both **absolute** and **periodic** values specified, then the **periodic** commands are evaluated only after the **absolute start** time is reached, and are not further evaluated after the **absolute end** time is reached.

The time-range feature relies on the system clock of the FWSM; however, the feature works best with NTP synchronization.

Examples

The following example shows how to restore the default behavior of the **absolute** keyword:

```
hostname(config-time-range)# default absolute
```

Related Commands

Command	Description
absolute	Defines an absolute time when a time range is in effect.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
time-range	Defines access control to the FWSM based on time.

default enrollment

To return all enrollment parameters to their system default values, use the **default enrollment** command in crypto ca trustpoint configuration mode.

default enrollment

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
Crypto ca trustpoint configuration	•	•	•	•	—

Command History	Release	Modification
	3.1(1)	This command was introduced.

Usage Guidelines Invocations of this command do not become part of the active configuration.

Examples The following example enters crypto ca trustpoint configuration mode for trustpoint central, and returns all enrollment parameters to their default values within trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# default enrollment
```

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

default-domain

To set a default domain name for users of the group policy, use the **default-domain** command in group-policy configuration mode. To delete a domain name, use the **no** form of this command.

default-domain {value *domain-name* | none}

no default-domain [*domain-name*]

Syntax Description

none	Indicates that there is no default domain name. Sets a default domain name with a null value, thereby disallowing a default domain name. Prevents inheriting a default domain name from a default or specified group policy.
value <i>domain-name</i>	Identifies the default domain name for the group.

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
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

You can use only alphanumeric characters, hyphens (-), and periods (.) in default domain names.

To delete all default domain names, use the **no** form of this command without arguments. This deletes all configured default domain names, including a null list created by issuing the **default-domain none** command.

To prevent users from inheriting a domain name, use the **default-domain none** command.

The FWSM passes the default domain name to the IPSec client to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets. When there are no default domain names, users inherit the default domain name in the default group policy.

Examples

The following example shows how to set a default domain name of FirstDomain for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

Related Commands

Command	Description
split-dns	Provides a list of domains to be resolved through the split tunnel.
split-tunnel-network-list	Identifies the access list the FWSM uses to distinguish networks that require tunneling and those that do not.
split-tunnel-policy	Lets an IPSec client conditionally direct packets over an IPSec tunnel in encrypted form, or to a network interface in cleartext form.

default-group-policy

To specify the set of attributes that the user inherits by default, use the **default-group-policy** command in tunnel-group general-attributes configuration mode. To eliminate a default group policy name, use the **no** form of this command.

default-group-policy *group-name*

no default-group-policy *group-name*

Syntax Description

group-name Specifies the name of the default group.

Defaults

The default group name is DfltGrpPolicy.

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
Tunnel-group general attributes configuration	•		•		

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The default group policy DfltGrpPolicy comes with the initial configuration of the FWSM. You can apply this attribute to all tunnel-group types.

Examples

The following example entered in config-general configuration mode, specifies a set of attributes for users to inherit by default for an IPSec LAN-to-LAN tunnel group named standard-policy. This set of commands defines the accounting server, the authentication server, the authorization server and the address pools.

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-general)# default-group-policy first-policy
hostname(config-general)# accounting-server-group aaa-server123
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)# authentication-server-group aaa-server456
hostname(config-general)# authorization-server-group aaa-server78
hostname(config-general)#
```

Related Commands	Command	Description
	clear-configure tunnel-group	Clears all configured tunnel groups.
	group-policy	Creates or edits a group policy.
	show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
	tunnel-group-map default group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

default-information (EIGRP)

To control the candidate default route information for the EIGRP routing process, use the **default-information** command in router configuration mode. To suppress EIGRP candidate default route information in incoming or outbound updates, use the **no** form of this command.

default-information {in | out} [*acl-name*]

no default-information {in | out}

Syntax Description

<i>acl-name</i>	(Optional) Named standard access list.
in	Configures EIGRP to accept exterior default routing information.
out	Configures EIGRP to advertise external routing information.

Defaults

Exterior routes are accepted and sent.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Only the **no** form of the command or **default-information** commands with an access list specified will appear in the running configuration because, by default, the candidate default routing information is accepted and sent. The **no** form of the command does not take an *acl-name* argument.

Examples

The following example disables the receipt of exterior or candidate default route information:

```
hostname(config)# router eigrp 100
hostname(config-router)# no default-information in
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

default-information originate

To generate a default external route into an OSPF routing domain, use the **default-information originate** command in router configuration mode. To disable this feature, use the **no** form of this command.

default-information originate [**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]

no default-information originate [[**always**] [**metric** *value*] [**metric-type** {**1** | **2**}] [**route-map** *name*]]

Syntax Description

always	(Optional) Always advertises the default route regardless of whether the software has a default route.
metric <i>value</i>	(Optional) Specifies the OSPF default metric value from 0 to 16777214.
metric-type { 1 2 }	(Optional) External link type associated with the default route advertised into the OSPF routing domain. Valid values are as follows: 1—Type 1 external route. 2—Type 2 external route.
route-map <i>name</i>	(Optional) Name of the route map to apply.

Defaults

The default values are as follows:

- metric** *value* is 1.
- metric-type** is 2.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

Using the **no** form of this command with optional keywords and arguments only removes the optional information from the command. For example, entering **no default-information originate metric 3** removes the **metric 3** option from the command in the running configuration. To remove the complete command from the running configuration, use the **no** form of the command without any options: **no default-information originate**.

Examples

The following example shows how to use the **default-information originate** command with an optional metric and metric type:

```
hostname(config-router)# default-information originate always metric 3 metric-type 2  
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.

default-metric

To specify the EIGRP metrics for redistributed routes, use the **default-metric** command in router configuration mode. To restore the default values, use the **no** form of this command.

default-metric *bandwidth delay reliability loading mtu*

no default-metric *bandwidth delay reliability loading mtu*

Syntax Description

<i>bandwidth</i>	The minimum bandwidth of the route in kilobytes per second. Valid values are from 1 to 4294967295.
<i>delay</i>	The route delay in tens of microseconds. Valid values are 1 to 4294967295.
<i>reliability</i>	The likelihood of successful packet transmission expressed as a number from 0 through 255. The value 255 means 100 percent reliability; 0 means no reliability.
<i>loading</i>	The effective bandwidth of the route expressed as a number from 1 to 255 (255 is 100 percent loading).
<i>mtu</i>	The smallest allowed value for the MTU, expressed in bytes. Valid values are from 1 to 65535.

Defaults

Only connected routes can be redistributed without a default metric. The metric of redistributed connected routes is set to 0.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You must use a default metric to redistribute a protocol into EIGRP unless you use the **metric** keyword and attributes in the **redistribute** command. Metric defaults have been carefully set to work for a wide variety of networks. Take great care when changing these values. Keeping the same metrics is supported only when you are redistributing from static routes.

Examples

The following example shows how the redistributed RIP route metrics are translated into EIGRP metrics with values as follows: bandwidth = 1000, delay = 100, reliability = 250, loading = 100, and MTU = 1500.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 172.16.0.0
hostname(config-router)# redistribute rip
hostname(config-router)# default-metric 1000 100 250 100 1500
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters router configuration mode for that process.
redistribute (EIGRP)	Redistributes routes into the EIGRP routing process.

delay

To set a delay value for an interface, use the **delay** command in interface configuration mode. To restore the default delay value, use the **no** form of this command.

delay *delay-time*

no delay

Syntax Description

<i>delay-time</i>	The delay time in tens of microseconds. Valid values are from 1 to 16777215.
-------------------	--

Defaults

The default delay depends upon the interface type. Use the **show interface** command to see the delay value for an interface.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The value entered is in tens of microseconds. The delay value displayed in the **show interface** output is in microseconds.

Examples

The following example changes the delay on an interface from the default 1000 to 2000. Truncated **show interface** command output is included before and after the **delay** command to show how the command affects the delay values. The delay value is noted in the second line of the **show interface** output, after the DLY label.

Notice that the command entered to change the delay value to 2000 is **delay 200**, not **delay 2000**. This is because the value entered with the **delay** command is in tens of microseconds, and the **show interface** output displays microseconds.

```
hostname(config)# show interface outside
Interface Vlan20 "outside", is up, line protocol is up
Hardware is EtherSVI, BW Unknown Speed-Capability, DLY 10 usec
MAC address 000f.23be.d980, MTU 1500
IP address 20.1.1.1, subnet mask 255.255.255.0
Traffic Statistics for "outside":
0 packets input, 0 bytes
```

 delay

```
0 packets output, 0 bytes
0 packets dropped
FWSM(config-if)#
```

Related Commands

Command	Description
show interface	Displays interface statistics and settings.

delete

To delete a file in the disk partition, use the **delete** command in privileged EXEC mode.

delete [/noconfirm] [/recursive] [disk:]*filename*

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
/recursive	(Optional) Deletes the specified file recursively in all subdirectories.
<i>filename</i>	Specifies the name of the file to delete.
disk:	Specifies the nonremovable internal Flash, followed by a colon.

Defaults

If you do not specify a directory, the directory is the current working directory 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
2.2(1)	This command was introduced.

Usage Guidelines

The file is deleted from the current working directory if a path is not specified. Wildcards are supported when deleting files. When deleting files, you are prompted with the filename and you must confirm the deletion.

The following example shows how to delete a file named *test.cfg* in the current working directory:

```
hostname# delete test.cfg
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
rmdir	Removes a file or directory.
show file	Displays the specified file.

deny

To deny traffic based on the application type, use the **deny** command in class configuration mode. You can access the class configuration mode by first entering the **policy-map** command. To remove the deny statement, use the **no** form of this command.

```
deny {all | protocol}
```

```
no deny {all | protocol}
```

Syntax Description

all	Specifies all protocols.
<i>protocol</i>	Specifies a specific protocol, by name or number. For a list of supported protocol names, use the deny ? command.

Defaults

By default, all protocols are permitted unless you specifically deny them.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The Programmable Intelligent Services Accelerator (PISA) on the switch can quickly determine the application type of a given flow by performing deep packet inspection. This determination can be made even if the traffic is not using standard ports. The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type.

Unlike the FWSM inspection feature, which passes through the control plane path, traffic that the PISA tags using GRE can pass through the FWSM accelerated path. Another benefit of FWSM and PISA integration is to consolidate your security configuration on a single FWSM instead of having to configure multiple upstream switches with PISAs installed.

You might want to deny certain types of application traffic when you want to preserve bandwidth for critical application types. For example, you might deny the use of peer-to-peer (P2P) applications if they are affecting your other critical applications.

After you identify the traffic using the **class-map** command, enter the **policy-map** command to identify the actions associated with each class map. Enter the **class** command to identify the class map, and then enter the **deny** command (along with **permit** commands) to determine the traffic to deny.

You can combine **permit** and **deny** statements to narrow the traffic that you want denied. You must enter at least one **deny** command. Unlike access lists, which have an implicit deny at the end, PISA actions have an implicit permit at the end.

For example, to permit all traffic except for Skype, eDonkey, and Yahoo, enter the following commands:

```
hostname(config-pmap-c)# deny skype
hostname(config-pmap-c)# deny yahoo
hostname(config-pmap-c)# deny eDonkey
```

The following example denies all traffic except for Kazaa and eDonkey:

```
hostname(config-pmap-c)# deny all
hostname(config-pmap-c)# permit kazaa
hostname(config-pmap-c)# permit eDonkey
```

See the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for detailed information about PISA integration, including essential information about configuring the switch to work with this feature.

Examples

The following is an example configuration for PISA integration:

```
hostname(config)# access-list BAD_APPS extended permit 10.1.1.0 255.255.255.0 10.2.1.0
255.255.255.0

hostname(config)# class-map denied_apps
hostname(config-cmap)# description "Apps to be blocked"
hostname(config-cmap)# match access-list BAD_APPS

hostname(config-cmap)# policy-map denied_apps_policy
hostname(config-pmap)# class denied_apps
hostname(config-pmap-c)# deny skype
hostname(config-pmap-c)# deny yahoo
hostname(config-pmap-c)# deny eDonkey

hostname(config-pmap-c)# service-policy denied_apps_policy inside
```

Related Commands

Command	Description
class	Identifies a class map in the policy map.
class-map	Creates a class map for use in a service policy.
permit	Permits PISA-tagged traffic.
policy-map	Configures a policy map that associates a class map and one or more actions.
service-policy	Assigns a policy map to an interface.
show conn	Shows connection information.

deny version

To deny a specific version of SNMP traffic, use the **deny version** command in snmp-map configuration mode, which is accessible by entering the **snmp-map** command from global configuration mode. To disable this command, use the **no** form of this command.

deny version *version*

no deny version *version*

Syntax Description

<i>version</i>	Specifies the version of SNMP traffic that the FWSM drops. The permitted values are 1 , 2 , 2c , and 3 .
----------------	--

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
snmp-map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **deny version** command to restrict SNMP traffic to specific versions of SNMP. Earlier versions of SNMP were less secure, so restricting SNMP traffic to Version 2 may be specified by your security policy. You use the **deny version** command within an SNMP map, which you configure using the **snmp-map** command. After creating the SNMP map, you enable the map using the **inspect snmp** command and then apply it to one or more interfaces using the **service-policy** command.

Examples

The following example shows how to identify SNMP traffic, define a SNMP map, define a policy, and apply the policy to the outside interface:

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
```

```
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect snmp	Enable SNMP application inspection.
policy-map	Associates a class map with specific security actions.
snmp-map	Defines an SNMP map and enables SNMP map configuration mode.
service-policy	Applies a policy map to one or more interfaces.

description

To add a description for a named configuration unit (for example, for a context or for an object group), use the **description** command in various configuration modes. To remove the description, use the **no** form of this command. The description adds helpful notes in your configuration.

description *text*

no description

Syntax Description

<i>text</i>	Sets the description as a text string up to 200 characters in length. If you want to include a question mark (?) in the string, you must type Ctrl-V before typing the question mark so you do not inadvertently invoke CLI help.
-------------	--

Defaults

No default behavior or values.

Command Modes

This command is available in various configuration modes.

Command History

Release	Modification
1.1(1)	This command was introduced.

Examples

The following example adds a description to the “Administration” context configuration:

```
hostname(config)# context administrator
hostname(config-ctx)# description This is the admin context.
hostname(config-ctx)# allocate-interface vlan 100
hostname(config-ctx)# allocate-interface vlan 200
hostname(config-ctx)# config-url disk://admin.cfg
```

Related Commands

Command	Description
class-map	Identifies traffic to which you apply actions in the policy-map command.
context	Creates a security context in the system configuration and enters context configuration mode.
interface	Configures an interface and enters interface configuration mode.
object-group	Identifies traffic to include in the access-list command.
policy-map	Identifies actions to apply to traffic identified by the class-map command.

dhcpd address

To define the IP address pool used by the DHCP server, use the **dhcpd address** command in global configuration mode. To remove an existing DHCP address pool, use the **no** form of this command.

dhcpd address *IP_address1*[-*IP_address2*] *interface_name*

no dhcpd address *interface_name*

Syntax Description

<i>interface_name</i>	Interface the address pool is assigned to.
<i>IP_address1</i>	Start address of the DHCP address pool.
<i>IP_address2</i>	End address of the DHCP address pool.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The **dhcpd address** *ip1*[-*ip2*] *interface_name* command specifies the DHCP server address pool. The address pool of a FWSM DHCP server must be within the same subnet of the FWSM interface on which it is enabled, and you must specify the associated FWSM interface using *interface_name*.

The size of the address pool is limited to 256 addresses per pool on the FWSM. If the address pool range is larger than 253 addresses, the netmask of the FWSM interface cannot be a Class C address (for example, 255.255.255.0) and needs to be something larger, for example, 255.255.254.0.

DHCP clients must be physically connected to the subnet of the FWSM DHCP server interface.

The **dhcpd address** command cannot use interface names with a “-” (dash) character because the “-” character is interpreted as a range specifier instead of as part of the object name.

The **no dhcpd address** *interface_name* command removes the DHCP server address pool that you configured for the specified interface.

Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for information on how to implement the DHCP server feature into the FWSM.

Examples

The following example shows how to use the **dhcpd address**, **dhcpd dns**, and **dhcpd enable** *interface_name* commands to configure an address pool and DNS server for the DHCP clients on the **dmz** interface of the FWSM:

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 209.165.200.226
hostname(config)# dhcpd enable dmz
```

The following example shows how to configure a DHCP server on the inside interface. It uses the **dhcpd address** command to assign a pool of 10 IP addresses to the DHCP server on that interface.

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd enable	Enables the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd dns

To define the DNS servers for DHCP clients, use the **dhcpd dns** command in global configuration mode. To clear defined servers, use the **no** form of this command.

dhcpd dns *dnsip1* [*dnsip2*]

no dhcpd dns [*dnsip1* [*dnsip2*]]

Syntax Description

<i>dnsip1</i>	IP address of the primary DNS server for the DHCP client.
<i>dnsip2</i>	(Optional) IP address of the alternate DNS server for the DHCP client.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The **dhcpd dns** command lets you specify the IP address or addresses of the DNS server(s) for the DHCP client. You can specify two DNS servers. The **no dhcpd dns** command lets you remove the DNS IP address(es) from the configuration.

Examples

The following example shows how to use the **dhcpd address**, **dhcpd dns**, and **dhcpd enable** *interface_name* commands to configure an address pool and DNS server for the DHCP clients on the **dmz** interface of the FWSM.

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 192.168.1.2
hostname(config)# dhcpd enable dmz
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd enable	Enables the DHCP server on the specified interface.
dhcpd wins	Defines the WINS servers for DHCP clients.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd domain

To define the DNS domain name for DHCP clients, use the **dhcpd domain** command in global configuration mode. To clear the DNS domain name, use the **no** form of this command.

dhcpd domain *domain_name*

no dhcpd domain [*domain_name*]

Syntax Description

domain_name The DNS domain name, for example example.com.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The **dhcpd domain** command lets you specify the DNS domain name for the DHCP client. The **no dhcpd domain** command lets you remove the DNS domain server from the configuration.

Examples

The following example shows how to use the **dhcpd domain** command to configure the domain name supplied to DHCP clients by the DHCP server on the FWSM:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd enable

To enable the DHCP server, use the **dhcpd enable** command in global configuration mode. To disable the DHCP server, use the **no** form of this command.

dhcpd enable *interface*

no dhcpd enable *interface*

Syntax Description

interface Specifies the interface on which to enable the DHCP server.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The DHCP server provides network configuration parameters to DHCP clients. Support for the DHCP server within the FWSM means that the FWSM can use DHCP to configure connected clients.

The **dhcpd enable interface** command lets you enable the DHCP daemon to listen for the DHCP client requests on the DHCP-enabled interface. The **no dhcpd enable** command disables the DHCP server feature on the specified interface.



Note

For multiple context mode, you cannot enable the DHCP server on an interface that is used by more than one context (a shared VLAN).

When the FWSM responds to a DHCP client request, it uses the IP address and subnet mask of the interface where the request was received as the IP address and subnet mask of the default gateway in the response.



Note

The FWSM DHCP server daemon does not support clients that are not directly connected to a FWSM interface.

Refer to the *Catalyst 6500 Series Switch and Cisco 7600 Series Router Firewall Services Module Configuration Guide* for information on how to implement the DHCP server feature into the FWSM.

Examples

The following example shows how to use the **dhcpd enable** command to enable the DHCP server on the inside interface:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
debug dhcpd	Displays debug information for the DHCP server.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd lease

To specify the DHCP lease length, use the **dhcpd lease** command in global configuration mode. To restore the default value for the lease, use the **no** form of this command.

dhcpd lease *lease_length*

no dhcpd lease [*lease_length*]

Syntax Description

<i>lease_length</i>	Length of the IP address lease, in seconds, granted to the DHCP client from the DHCP server; valid values are from 300 to 1048575 seconds.
---------------------	--

Defaults

The default *lease_length* is 3600 seconds.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The **dhcpd lease** command lets you specify the length of the lease, in seconds, that is granted to the DHCP client. This lease indicates how long the DHCP client can use the assigned IP address that the DHCP server granted.

The **no dhcpd lease** command lets you remove the lease length that you specified from the configuration and replaces this value with the default value of 3600 seconds.

Examples

The following example shows how to use the **dhcpd lease** command to specify the length of the lease of DHCP information for DHCP clients:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd option

To configure DHCP options, use the **dhcpd option** command in global configuration mode. To clear the option, use the **no** form of this command. You can use the **dhcpd option** command to provide TFTP server information to Cisco IP Phones and routers.

dhcpd option *code* { **ascii** *string* } | { **ip** *IP_address* [*IP_address*] } | { **hex** *hex_string* }

no dhcpd option *code*

Syntax Description

ascii	Specifies that the option parameter is an ASCII character string.
<i>code</i>	A number representing the DHCP option being set. Valid values are 0 to 255. See the “Usage Guidelines” section, below, for the list of DHCP option codes that are not supported.
hex	Specifies that the option parameter is a hexadecimal string.
<i>hex_string</i>	Specifies a hexadecimal string with an even number of digits and no spaces. You do not need to use a 0x prefix.
ip	Specifies that the option parameter is an IP address. You can specify a maximum of two IP addresses with the ip keyword.
<i>IP_address</i>	Specifies a dotted-decimal IP address.
<i>string</i>	Specifies an ASCII character string without spaces.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

When a DHCP option request arrives at the FWSM DHCP server, the FWSM places the value or values that are specified by the **dhcpd option** command in the response to the client.

The **dhcpd option 66** and **dhcpd option 150** commands specify TFTP servers that Cisco IP Phones and routers can use to download configuration files. Use the commands as follows:

- **dhcpd option 66** *ascii string*, where *string* is either the IP address or hostname of the TFTP server. Only one TFTP server can be specified for option 66.
- **dhcpd option 150** *ip IP_address [IP_address]*, where *IP_address* is the IP address of the TFTP server. You can specify a maximum of two IP addresses for option 150.

**Note**

The **dhcpd option 66** command only takes an **ascii** parameter, and the **dhcpd option 150** only takes an **ip** parameter.

Use the following guidelines when specifying an IP address for the **dhcpd option 66 | 150** commands:

- If the TFTP server is located on the DHCP server interface, use the local IP address of the TFTP server.
- If the TFTP server is located on a less secure interface than the DHCP server interface, then general outbound rules apply. Create a group of NAT, global, and **access-list** entries for the DHCP clients, and use the actual IP address of the TFTP server.
- If the TFTP server is located on a more secure interface, then general inbound rules apply. Create a group of static and **access-list** statements for the TFTP server and use the global IP address of the TFTP server.

For information about other DHCP options, refer to RFC 2132.

**Note**

The security appliance does not verify that the option type and value that you provide match the expected type and value for the option code as defined in RFC 2132. For example, you can enter **dhcpd option 46 ascii hello**, and the security appliance accepts the configuration although option 46 is defined in RFC 2132 as expecting a single-digit, hexadecimal value.

You cannot configure the following DHCP options with the **dhcpd option** command:

Option Code	Description
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

Examples

The following example shows how to specify a TFTP server for DHCP option 66:

```
hostname(config)# dhcpd option 66 ascii MyTftpServer
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd ping-timeout

To change the default timeout for DHCP ping, use the **dhcpd ping-timeout** command in global configuration mode. To return to the default value, use the **no** form of this command. To avoid address conflicts, the DHCP server sends two ICMP ping packets to an address before assigning that address to a DHCP client. This command specifies the ping timeout in milliseconds.

dhcpd ping-timeout *number*

no dhcpd ping-timeout

Syntax Description

number The timeout value of the ping, in milliseconds. The minimum value is 10, the maximum is 10000. The default is 50.

Defaults

The default number of milliseconds for *number* is 50.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The FWSM waits for both ICMP ping packets to time out before assigning an IP address to a DHCP client. For example, if the default value is used, the FWSM waits for 1500 milliseconds (750 milliseconds for each ICMP ping packet) before assigning an IP address.

A long ping timeout value can adversely affect the performance of the DHCP server.

Examples

The following example shows how to use the **dhcpd ping-timeout** command to change the ping timeout value for the DHCP server:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping-timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcpd wins

To define the WINS servers for DHCP clients, use the **dhcpd wins** command in global configuration mode. To remove the WINS servers from the DHCP server, use the **no** form of this command.

dhcpd wins *server1* [*server2*]

no dhcpd wins [*server1* [*server2*]]

Syntax Description

<i>server1</i>	Specifies the IP address of the primary Microsoft NetBIOS name server (WINS server).
<i>server2</i>	(Optional) Specifies the IP address of the alternate Microsoft NetBIOS name server (WINS server).

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
1.1(1)	This command was introduced.
3.1(1)	This command was changed from dhcpd .

Usage Guidelines

The **dhcpd wins** command lets you specify the addresses of the WINS servers for the DHCP client. The **no dhcpd wins** command removes the WINS server IP addresses from the configuration.

Examples

The following example shows how to use the **dhcpd wins** command to specify WINS server information that is sent to DHCP clients:

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

Related Commands

Command	Description
clear configure dhcpd	Removes all DHCP server settings.
dhcpd address	Specifies the address pool used by the DHCP server on the specified interface.
dhcpd dns	Defines the DNS servers for DHCP clients.
show dhcpd	Displays DHCP binding, statistic, or state information.
show running-config dhcpd	Displays the current DHCP server configuration.

dhcp-network-scope

To specify the range of IP addresses the FWSM DHCP server should use to assign addresses to users of this group policy, use the **dhcp-network-scope** 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 value from another group policy. To prevent inheriting a value, use the **dhcp-network-scope none** command.

dhcp-network-scope {*ip_address*} | none

no dhcp-network-scope

Syntax Description

<i>ip_address</i>	Specifies the IP subnetwork the DHCP server should use to assign IP addresses to users of this group policy.
none	Sets the DHCP subnetwork to a null value, thereby allowing no IP addresses. 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:

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example shows how to set an IP subnetwork of 10.10.85.0 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dhcp-network-scope 10.10.85.0
```

dhcprelay enable

To enable the DHCP relay agent, use the **dhcprelay enable** command in global configuration mode. To disable DHCP relay agent, use the **no** form of this command. The DHCP relay agent allows DHCP requests to be forwarded from a specified FWSM interface to a specified DHCP server.

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

Syntax Description

<i>interface_name</i>	Name of the interface on which the DHCP relay agent accepts client requests.
-----------------------	--

Defaults

The DHCP relay agent is disabled.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

Usage Guidelines

For the FWSM to start the DHCP relay agent with the **dhcprelay enable** *interface_name* command, you must have a **dhcprelay server** command already in the configuration. Otherwise, the FWSM displays an error message similar to the following:

```
DHCPRA: Warning - There are no DHCP servers configured!
          No relaying can be done without a server!
          Use the 'dhcprelay server <server_ip> <server_interface>' command
```

You cannot enable DHCP relay under the following conditions:

- You cannot enable DHCP relay and the DHCP relay server on the same interface.
- You cannot enable DHCP relay and a DHCP server (**dhcpd enable**) on the same interface.
- You cannot enable DHCP relay in a context at the same time as the DHCP server.
- For multiple context mode, you cannot enable DHCP relay on an interface that is used by more than one context (a shared VLAN).

The **no dhcprelay enable** *interface_name* command removes the DHCP relay agent configuration for the interface that is specified by *interface_name* only.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the FWSM, client requests on the inside interface of the FWSM, and a timeout value up to 90 seconds:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

The following example shows how to disable the DHCP relay agent:

```
hostname(config)# no dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
debug dhcp relay	Displays debug information for the DHCP relay agent.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay information trust

You can preserve option 82 and forward a packet by identifying an interface as a trusted interface thus ensuring that DHCP snooping and IP source guard features on the switch work along with the FWSM.

You can enable this feature on interfaces configured with IPv4 and IPv6 addresses.

To configure a particular interface as a trusted interface that preserves option 82, enter the following command:

dhcprelay information trusted

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
4.0	This command was introduced.

Usage Guidelines

The interface-specific trusted configuration and global trusted configuration can exist together. For example there are three interfaces A, B and C, and a user configures interface A as trusted using the interface-specific command. Then the user configures the global command also.

Now all the three interfaces A, B, and C are trusted interfaces. If you enter the no dhcprelay information trust-all command, then interfaces B and C will become non-trusted interfaces. Interface A will continue to be a trusted interface, since the interface-specific trusted configuration is not removed.

Examples

The following example enables a particular interface as a trusted interface:

```
hostname(config)# dhcprelay information trusted
```

Related Commands

Command	Description
dhcprelay information trust-all	To configure all interfaces as trusted interfaces.

dhcprelay information trust-all

You can preserve option 82 and forward packets by identifying all the interfaces as trusted interfaces and ensuring that DHCP snooping and IP source guard features on the switch work along with the FWSM.

You can enable this feature on interfaces configured with IPv4 and IPv6 addresses.

To configure all interfaces as trusted interfaces, enter the following command:

dhcprelay information trust-all

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
Global configuration	•	—	•	•	—

Command History

Release	Modification
4.0	This command was introduced.

Usage Guidelines

The interface-specific trusted configuration and global trusted configuration can exist together. For example there are three interfaces A, B and C, and a user configures interface A as trusted using the interface-specific command. Then the user configures the global command also.

Now all the three interfaces A, B, and C are trusted interfaces. If you enter the no dhcprelay information trust-all command, then interfaces B and C will become non-trusted interfaces. Interface A will continue to be a trusted interface, since the interface-specific trusted configuration is not removed.

Examples

The following example enables all interfaces except the interfaces that are shared or configured for the DHCP server:

```
hostname(config)# dhcprelay information trust-all
```

Related Commands

Command	Description
dhcprelay information trusted	To configure specific interfaces as trusted interfaces.

dhcprelay server

To specify the DHCP server that DHCP requests are forwarded to, use the **dhcprelay server** command in global configuration mode. To remove the DHCP server from the DHCP relay configuration, use the **no** form of this command. The DHCP relay agent allows DHCP requests to be forwarded from a specified FWSM interface to a specified DHCP server.

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address [interface_name]*

Syntax Description

<i>interface_name</i>	Name of the FWSM interface on which the DHCP server resides.
<i>IP_address</i>	The IP address of the DHCP server to which the DHCP relay agent forwards client DHCP requests.

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
Global configuration	•	—	•	•	—

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

Usage Guidelines

You can add up to four DHCP relay servers per interface; however, there is a limit of ten DHCP relay servers total that can be configured on the FWSM. You must add at least one **dhcprelay server** command to the FWSM configuration before you can enter the **dhcprelay enable** command. You cannot configure a DHCP client on an interface that has a DHCP relay server configured.

The **dhcprelay server** command opens UDP port 67 on the specified interface and starts the DHCP relay task as soon as the **dhcprelay enable** command is added to the configuration. If there is **no dhcprelay enable** command in the configuration, then the sockets are not opened and the DHCP relay task does not start.

When you use the **no dhcprelay server** *IP_address [interface_name]* command, the interface stops forwarding DHCP packets to that server.

The **no dhcprelay server** *IP_address [interface_name]* command removes the DHCP relay agent configuration for the DHCP server that is specified by *IP_address [interface_name]* only.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the FWSM, client requests on the inside interface of the FWSM, and a timeout value up to 90 seconds:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay setroute

To set the default gateway address in the DHCP reply, use the **dhcprelay setroute** command in global configuration mode. To remove the default router, use the **no** form of this command. This command causes the default IP address of the DHCP reply to be substituted with the address of the specified FWSM interface.

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

Syntax Description

interface Configures the DHCP relay agent to change the first default IP address (in the packet sent from the DHCP server) to the address of *interface*.

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
Global configuration	•	—	•	•	—

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

Usage Guidelines

The **dhcprelay setroute** *interface* command lets you enable the DHCP relay agent to change the first default router address (in the packet sent from the DHCP server) to the address of *interface*.

If there is no default router option in the packet, the FWSM adds one containing the address of *interface*. This action allows the client to set its default route to point to the FWSM.

When you do not configure the **dhcprelay setroute** *interface* command (and there is a default router option in the packet), it passes through the FWSM with the router address unaltered.

Examples

The following example shows how to use the **dhcprelay setroute** command to set the default gateway in the DHCP reply from the external DHCP server to the inside interface of the FWSM:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay setroute inside
hostname(config)# dhcprelay enable inside
```

Related Commands	Command	Description
	clear configure dhcprelay	Removes all DHCP relay agent settings.
	dhcprelay enable	Enables the DHCP relay agent on the specified interface.
	dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
	dhcprelay timeout	Specifies the timeout value for the DHCP relay agent.
	show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcprelay timeout

To set the DHCP relay agent timeout value, use the **dhcprelay timeout** command in global configuration mode. To restore the timeout value to its default value, use the **no** form of this command.

dhcprelay timeout *seconds*

no dhcprelay timeout

Syntax Description

<i>seconds</i>	Specifies the number of seconds that are allowed for DHCP relay address negotiation.
----------------	--

Defaults

The default value for the dhcprelay timeout is 60 seconds.

Command Modes

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

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

Command History

Release	Modification
2.2(1)	This command was introduced.
3.1(1)	This command was changed from dhcprelay .

Usage Guidelines

The **dhcprelay timeout** command lets you set the amount of time, in seconds, allowed for responses from the DHCP server to pass to the DHCP client through the relay binding structure.

Examples

The following example shows how to configure the DHCP relay agent for a DHCP server with an IP address of 10.1.1.1 on the outside interface of the FWSM, client requests on the inside interface of the FWSM, and a timeout value up to 90 seconds:

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

Related Commands

Command	Description
clear configure dhcprelay	Removes all DHCP relay agent settings.
dhcprelay enable	Enables the DHCP relay agent on the specified interface.
dhcprelay server	Specifies the DHCP server that the DHCP relay agent forwards DHCP requests to.
dhcprelay setroute	Defines IP address that the DHCP relay agent uses as the default router address in DHCP replies.
show running-config dhcprelay	Displays the current DHCP relay agent configuration.

dhcp-server

To configure support for DHCP servers that assign IP addresses to clients as a VPN tunnel is established, use the **dhcp-server** command in tunnel-group general-attributes configuration mode. To return this command to the default, use the **no** form of this command.

dhcp-server *hostname1* [...*hostname10*]

no dhcp-server *hostname*

Syntax Description

<i>hostname1</i>	Specifies the IP address of the DHCP server. You can specify up to 10
<i>...hostname10</i>	DHCP servers.

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
Tunnel-group general attributes configuration	•		•		

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

In interface level, enter the **dhcp-server** <ip_address> command. There is no need to add <interface> in the command.

You can apply this attribute to IPSec remote access tunnel-group types only.

Examples

The following command entered in config-general configuration mode, adds three DHCP servers (dhcp1, dhcp2, and dhcp3) to the IPSec remote-access tunnel group remotegrp:

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-general)# default-group-policy remotegrp
hostname(config-general)# dhcp-server dhcp1 dhcp2 dhcp3
hostname(config-general)
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group-map default group	Associates the certificate map entries created using the crypto ca certificate map command with tunnel groups.

dir

To display the directory contents, use the **dir** command in privileged EXEC mode.

dir [/all] [all-file systems] [/recursive] [flash: | system:] [path]

Syntax Description

/all	(Optional) Displays all files.
all-file systems	(Optional) Displays the files of all file systems
/recursive	(Optional) Displays the directory contents recursively.
system:	(Optional) Displays the directory contents of the file system.
flash:	(Optional) Displays the directory contents of the default Flash partition.
path	(Optional) Specifies a specific path.

Defaults

If you do not specify a directory, the directory is the current working directory by default.

Command Modes

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

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

Command History

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

Usage Guidelines

The **dir** command without keywords or arguments displays the directory contents of the current directory.

Examples

The following example shows how to display the directory contents:

```
hostname# dir
Directory of disk0:/

 1      -rw-  1519      10:03:50 Jul 14 2003    my_context.cfg
 2      -rw-  1516      10:04:02 Jul 14 2003    my_context.cfg
 3      -rw-  1516      10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

This example shows how to display recursively the contents of the entire file system:

```
hostname# dir /recursive disk0:
Directory of disk0:/*
 1      -rw-  1519      10:03:50 Jul 14 2003    my_context.cfg
```

```
2      -rw-  1516      10:04:02 Jul 14 2003  my_context.cfg
3      -rw-  1516      10:01:34 Jul 14 2003  admin.cfg
60985344 bytes total (60973056 bytes free)
```

Related Commands

Command	Description
cd	Changes the current working directory to the one specified.
pwd	Displays the current working directory.
mkdir	Creates a directory.
rmdir	Removes a directory.

disable

To exit privileged EXEC mode and return to unprivileged EXEC mode, use the **disable** command in privileged EXEC mode.

disable

Syntax Description This command has no arguments or keywords.

Defaults No default behaviors or values.

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

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

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines Use the **enable** command to enter privileged EXEC mode. The **disable** command lets you exit privileged EXEC mode and returns you to user EXEC mode.

Examples The following example shows how to enter privileged EXEC mode:

```
hostname> enable
hostname#
```

The following example shows how to exit privileged EXEC mode:

```
hostname# disable
hostname>
```

Command	Description
enable	Enables privileged EXEC mode.

distance eigrp

To configure the administrative distances of internal and external EIGRP routes, use the **distance eigrp** command in router configuration mode. To restore the default values, use the **no** form of this command.

distance eigrp *internal-distance external-distance*

no distance eigrp

Syntax Description

<i>external-distance</i>	Administrative distance for EIGRP external routes. External routes are those for which the best path is learned from a neighbor external to the autonomous system. Valid values are from 1 to 255.
<i>internal-distance</i>	Administrative distance for EIGRP internal routes. Internal routes are those that are learned from another entity within the same autonomous system. Valid values are from 1 to 255.

Defaults

The default values are as follows:

- *external-distance* is 170
- *internal-distance* is 90

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

Because every routing protocol has metrics based on algorithms that are different from the other routing protocols, it is not always possible to determine the “best path” for two routes to the same destination that were generated by different routing protocols. Administrative distance is a route parameter that the FWSM uses to select the best path when there are two or more different routes to the same destination from two different routing protocols.

If you have more than one routing protocol running on the FWSM, you can use the **distance eigrp** command to adjust the default administrative distances of routes discovered by the EIGRP routing protocol in relation to the other routing protocols. [Table 11-1](#) lists the default administrative distances for the routing protocols supported by the FWSM.

Table 11-1 *Default Administrative Distances*

Route Source	Default Administrative Distance
Connected interface	0
Static route	1
EIGRP summary route	5
Internal EIGRP	90
OSPF	110
RIP	120
EIGRP external route	170
Unknown	255

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for both internal and external EIGRP routes.

Examples

The following example uses the **distance eigrp** command set the administrative distance of all EIGRP internal routes to 80 and all EIGRP external routes to 115. Setting the EIGRP external route administrative distance to 115 would give routes discovered by EIGRP to a specific destination preference over the same routes discovered by RIP but not by OSPF.

```
hostname(config)# router eigrp 100
hostname(config-router)# network 192.168.7.0
hostname(config-router)# network 172.16.0.0
hostname(config-router)# distance eigrp 90 115
```

Related Commands

Command	Description
router eigrp	Creates an EIGRP routing process and enters configuration mode for that process.

distance ospf

To define OSPF route administrative distances based on route type, use the **distance ospf** command in router configuration mode. To restore the default values, use the **no** form of this command.

distance ospf [*intra-area d1*] [*inter-area d2*] [*external d3*]

no distance ospf

Syntax Description

<i>d1</i> , <i>d2</i> , and <i>d3</i>	Distance for each route types. Valid values range from 1 to 255.
external	(Optional) Sets the distance for routes from other routing domains that are learned by redistribution.
inter-area	(Optional) Sets the distance for all routes from one area to another area.
intra-area	(Optional) Sets the distance for all routes within an area.

Defaults

The default values for *d1*, *d2*, and *d3* are 110.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

You must specify at least one keyword and argument. You can enter the commands for each type of administrative distance separately, however they appear as a single command in the configuration. If you reenter an administrative distance, the administrative distance for only that route type changes; the administrative distances for any other route types remain unaffected.

The **no** form of the command does not take any keywords or arguments. Using the **no** form of the command restores the default administrative distance for all of the route types. If you want to restore the default administrative distance for a single route type when you have multiple route types configured, you can do one of the following:

- Manually set that route type to the default value.
- Use the **no** form of the command to remove the entire configuration and then reenter the configurations for the route types you want to keep.

Examples

The following example sets the administrative distance of external routes to 150:

```
hostname(config-router)# distance ospf external 105
hostname(config-router)#
```

The following example shows how entering separate commands for each route type appears as a single command in the router configuration:

```
hostname(config-router)# distance ospf intra-area 105 inter-area 105
hostname(config-router)# distance ospf intra-area 105
hostname(config-router)# distance ospf external 105
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
  distance ospf intra-area 105 inter-area 105 external 105
!
hostname(config)#
```

The following example shows how to set each administrative distance to 105, and then change only the external administrative distance to 150. The **show running-config router ospf** command shows how only the external route type value changed, while the other route types retained the value previously set.

```
hostname(config-router)# distance ospf external 105 intra-area 105 inter-area 105
hostname(config-router)# distance ospf external 150
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
  distance ospf intra-area 105 inter-area 105 external 150
!
hostname(config)#
```

Related Commands

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

distribute-list in

To filter the networks received in routing updates, use the **distribute-list in** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **in** [**interface** *if_name*]

no distribute-list *acl* **in** [**interface** *if_name*]

Syntax Description

<i>acl</i>	Name of a standard access list.
<i>if_name</i>	(Optional) The interface name as specified by the nameif command. Specifying an interface causes the access list to be applied only to routing updates received on that interface.

Defaults

Networks are not filtered in incoming updates.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If no interface is specified, the access list will be applied to all incoming updates.

Examples

The following example filters EIGRP routing updates received on the outside interface. It accepts routes in the 10.0.0.0 network and discards all others.

```
hostname(config)# access-list eigrp_filter permit 10.0.0.0
hostname(config)# access-list eigrp_filter deny any
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list eigrp_filter in interface outside
```

Related Commands

Command	Description
distribute-list out	Filters networks from being advertised in routing updates.

Command	Description
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

distribute-list out

To filter specific networks from being sent in routing updates, use the **distribute-list out** command in router configuration mode. To remove the filtering, use the **no** form of this command.

distribute-list *acl* **out** [**interface** *if_name* | **ospf** *pid* | **static** | **connected**]

no distribute-list *acl* **out** [**interface** *if_name* | **ospf** *pid* | **static** | **connected**]

Syntax Description

<i>acl</i>	Name of a standard access list.
connected	(Optional) Filters only connected routes.
interface <i>if_name</i>	(Optional) The interface name as specified by the nameif command. Specifying an interface causes the access list to be applied only to routing updates sent on the specified interface.
ospf <i>pid</i>	(Optional) Filters only OSPF routes discovered by the specified OSPF process.
static	(Optional) Filters only static routes.

Defaults

Networks are not filtered in sent updates.

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
Router configuration	•	—	•	—	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If no interface is specified, the access list will be applied to all outgoing updates.



Note

OSPF routes cannot be filtered from entering the OSPF database. The **distribute-list out** command works only on the routes being redistributed by the Autonomous System Boundary Routers (ASBRs) into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and interarea routes.

Examples

The following example would cause only one network to be advertised by a RIP routing process, network 10.108.0.0:

```
hostname(config)# access-list 1 permit 10.108.0.0  
hostname(config)# access-list 1 deny 0.0.0.0 255.255.255.255  
hostname(config)# router rip  
hostname(config-router)# network 10.108.0.0  
hostname(config-router)# distribute-list 1 out
```

Related Commands

Command	Description
distribute-list in	Filters networks received in routing updates.
router eigrp	Enters router configuration mode for the EIGRP routing process.
show running-config router	Displays the commands in the global router configuration.

dns domain-lookup

To enable the FWSM to send DNS requests to a DNS server to perform a name lookup for supported commands, use the **dns domain-lookup** command in global configuration mode. To disable DNS lookup, use the **no** form of this command.

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

Syntax Description

interface_name Specifies the interface on which you want to enable DNS lookup. If you enter this command multiple times to enable DNS lookup on multiple interfaces, the FWSM tries each interface in order until it receives a response.

Defaults

DNS lookup is disabled by default.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **dns name-server** command to configure the DNS server addresses to which you want to send DNS requests. See the **dns name-server** command for a list of commands that support DNS lookup.

The FWSM maintains a cache of name resolutions that consists of dynamically learned entries. Instead of making queries to external DNS servers each time an hostname-to-IP-address translation is needed, the FWSM caches information returned from external DNS requests. The FWSM only makes requests for names that are not in the cache. The cache entries time out automatically according to the DNS record expiration, or after 72 hours, whichever comes first.

Examples

The following example enables DNS lookup on the inside interface:

```
hostname(config)# dns domain-lookup inside
```

Related Commands

Command	Description
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the FWSM does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns name-server

To identify one or more DNS servers, use the **dns name-server** command in global configuration mode. To remove a server, use the **no** form of this command.

[no] dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

Syntax Description

ip_address Specifies the DNS server IP address. You can specify up to six addresses as separate commands, or for convenience, up to six addresses in one command separated by spaces. If you enter multiple servers in one command, the FWSM saves each server in a separate command in the configuration. The FWSM tries each DNS server in order until it receives a response.

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
Global configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The FWSM uses DNS to resolve server names in your certificate configuration. Other features that define server names (such as AAA) do not support DNS resolution. You must enter the IP address or manually resolve the name to an IP address by using the **name** command.

To enable DNS lookup, configure the **dns domain-lookup** command. If you do not enable DNS lookup, the DNS servers are not used.

Commands that support DNS resolution include the following:

- **enrollment url**
- **url**

You can manually enter names and IP addresses using the **name** command.

See the **dns retries** command to set how many times the FWSM tries the list of DNS servers.

Examples

The following example shows how to add three DNS servers:

```
hostname(config)-if# dns name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

The following output shows how the FWSM saves the configuration as separate commands:

```
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
```

The following example shows how to add two additional servers as one command:

```
hostname(config-if)# dns name-server 10.5.1.1 10.8.3.8
hostname(config-if)# show running-config dns
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
dns name-server 10.5.1.1
dns name-server 10.8.3.8
...
```

The following example shows how to enter the servers using two commands:

```
hostname(config)# dns name-server 10.5.1.1
hostname(config)# dns name-server 10.8.3.8
```

The following example shows how to delete multiple servers using one command. You can also use multiple commands.

```
hostname(config)# no dns name-server 10.5.1.1 10.8.3.8
```

Related Commands

Command	Description
dns domain-lookup	Enables the FWSM to perform a name lookup.
dns retries	Specifies the number of times to retry the list of DNS servers when the FWSM does not receive a response.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns retries

To specify the number of times to retry the list of DNS servers when the FWSM does not receive a response, use the **dns retries** command in global configuration mode. To restore the default setting, use the **no** form of this command.

dns retries *number*

no dns retries [*number*]

Syntax Description

number Specifies the number of retries between 0 and 10. The default is 2.

Defaults

The default number of retries is 2.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Add DNS servers using the **dns name-server** command.

Examples

The following example sets the number of retries to 0. The FWSM only tries each server one time.

```
hostname(config)# dns retries 0
```

Related Commands

Command	Description
dns domain-lookup	Enables the FWSM to perform a name lookup.
dns name-server	Configures a DNS server address.
dns timeout	Specifies the amount of time to wait before trying the next DNS server.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns timeout

To specify the amount of time to wait before trying the next DNS server, use the **dns timeout** command in global configuration mode. To restore the default timeout, use the **no** form of this command.

dns timeout *seconds*

no dns timeout [*seconds*]

Syntax Description

seconds Specifies the timeout in seconds between 1 and 30. The default is 2 seconds. Each time the FWSM retries the list of servers, this timeout doubles. See the **dns retries** command to configure the number of retries.

Defaults

The default timeout is 2 seconds.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Examples

The following example sets the timeout to 1 second:

```
hostname(config)# dns timeout 1
```

Related Commands

Command	Description
dns name-server	Configures a DNS server address.
dns retries	Specifies the number of times to retry the list of DNS servers when the FWSM does not receive a response.
dns domain-lookup	Enables the FWSM to perform a name lookup.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

dns-guard

To <text>, use the **dns-guard** command in global configuration mode.

To <text about removing command>, use the **no** form of this command.

dns-guard

no dns-guard

Syntax Description

There are no arguments or keywords for this command.

Defaults

DNS Guard is enabled by default.

Command Modes

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

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

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When a client sends a DNS request to an external DNS server, only the first response is accepted by the FWSM. All additional responses from other DNS servers are dropped by the FWSM.

After the client issues a DNS request, a dynamic hole allows UDP packets to return from the DNS server. When the FWSM receives a response from the first DNS server, the connection that was created in the accelerated path is dropped so that subsequent responses from other DNS servers are dropped by the FWSM. The UDP DNS connection is deleted immediately rather than marking the connection for deletion.

The FWSM creates a session-lookup key based on the source and destination IP address along with the protocol and the DNS ID instead of the source and destination ports.

If the DNS client and DNS server use TCP for DNS, the connection is cleared like a normal TCP connection.

However, if clients receive DNS responses from multiple DNS servers, you can disable the default DNS behavior on a per context basis. When DNS Guard is disabled, a response from the first DNS server does not delete the connection and the connection is treated as a normal UDP connection.

Examples

The following example shows the use of the **dns-guard** command to disable the DNS Guard feature:

```
hostname(config)# no dns-guard
```

```
hostname(config)# show running-config | inc dns-guard
no dns-guard
hostname(config)#
```

Related Commands

Command	Description
<code>inspect dns</code>	Enables inspection of DNS application traffic.

dns-server

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

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

no dns-server

Syntax Description

none	Sets dns-servers to a null value, thereby allowing no DNS servers. Prevents inheriting a value from a default or specified group policy.
value <i>ip_address</i>	Specifies the IP address of the primary and secondary DNS servers.

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
Group-policy configuration	•	—	•	—	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example shows how to configure DNS 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)# dns-server value 10.10.10.15 10.10.10.30 10.10.10.45
```


domain-name

To set the default domain name, use the **domain-name** command in global configuration mode. To remove the domain name, use the **no** form of this command.

domain-name *name*

no domain-name [*name*]

Syntax Description

name Sets the domain name, up to 63 characters.

Defaults

The default domain name is default.domain.invalid.

Command Modes

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

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

Command History

Release	Modification
1.1(1)	This command was introduced.

Usage Guidelines

The FWSM appends the domain name as a suffix to unqualified names. For example, if you set the domain name to “example.com,” and specify a syslog server by the unqualified name of “jupiter,” then the security appliance qualifies the name to “jupiter.example.com.”

For multiple context mode, you can set the domain name for each context, as well as within the system execution space.

Examples

The following example sets the domain as example.com:

```
hostname(config)# domain-name example.com
```

Related Commands

Command	Description
dns domain-lookup	Enables the FWSM to perform a name lookup.
dns name-server	Configures a DNS server address.

Command	Description
hostname	Sets the FWSM hostname.
show running-config domain-name	Shows the domain name configuration.

drop (class)

To drop all packets that match the **match** command or **class** command, use the **drop** command in match or class configuration mode. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. To disable this action, use the **no** form of this command.

drop [log]

no drop [log]

Syntax Description

log	Logs the match. The system log message number depends on the application.
------------	---

Defaults

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

When using the Modular Policy Framework, drop packets that match a **match** command or class map by using the **drop** command in match or class configuration mode. This drop action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action.

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop** command to drop all packets that match the **match** command or **class** command.

If you drop a packet, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http** *http_policy_map* command where *http_policy_map* is the name of the inspection policy map.

Examples

The following example drops packets and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

Related Commands

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

drop (gtp-map)

To drop specified GTP messages, use the **drop** command in gtp-map configuration mode. To remove the command, use the **no** form of this command.

drop {**apn** *access_point_name* | **message** *message_id* | **version** *version*}

no drop {**apn** *access_point_name* | **message** *message_id* | **version** *version*}

Syntax Description

apn	Drops GTP messages with the specified access point name.
<i>access_point_name</i>	The text string of the APN which will be dropped.
message	Drops specific GTP messages.
<i>message_id</i>	An alphanumeric identifier for the message that you want to drop. The valid range for <i>message_id</i> is 1 to 255.
version	Drops GTP messages with the specified version.
<i>version</i>	Use 0 to identify Version 0 and 1 to identify Version 1. Version 0 of GTP uses port 2123, while Version 1 uses port 3386.

Defaults

All messages with valid message IDs, APNs, and version are inspected.

Any APN is allowed.

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
Gtp-map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

Use the **drop message** command to drop specific GTP messages that you do not want to allow in your network.

Use the **drop apn** command to drop GTP messages with the specified access point. Use the **drop version** command to drop GTP messages with the specified version.

Examples

The following example drops traffic to message ID 20:

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# drop message 20
```

Related Commands	Commands	Description
	clear service-policy inspect gtp	Clears global GTP statistics.
	debug gtp	Displays detailed information about GTP inspection.
	gtp-map	Defines a GTP map and enables GTP map configuration mode.
	inspect gtp	Applies a specific GTP map to use for application inspection.
	show service-policy inspect gtp	Displays the GTP configuration.

drop-connection

When using the Modular Policy Framework, drop packets and close the connection for traffic that matches a **match** command or class map by using the **drop-connection** command in match or class configuration mode. You can access the match or class configuration mode by first entering the **policy-map type inspect** command. To disable this action, use the **no** form of this command.

drop-connection [**log**]

no drop-connection [**log**]

Syntax Description

log	Logs the match. The system log message number depends on the application.
------------	---

Defaults

No default behaviors or values.

Command Modes

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

Command Mode	Firewall Mode		Security Context		
	Routed	Transparent	Single	Multiple Context	System
Match and class configuration	•	•	•	•	—

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The connection will be removed from the connection database on the FWSM. Any subsequent packets entering the FWSM for the dropped connection will be discarded. This drop-connection action is available in an inspection policy map for application traffic; however, not all applications allow this action.

An inspection policy map consists of one or more **match** and **class** commands. The exact commands available for an inspection policy map depends on the application. After you enter the **match** or **class** command to identify application traffic (the **class** command refers to an existing **class-map type inspect** command that in turn includes **match** commands), you can enter the **drop-connection** command to drop packets and close the connection for traffic that matches the **match** command or **class** command.

If you drop a packet or close a connection, then no further actions are performed in the inspection policy map. For example, if the first action is to drop the packet and close the connection, then it will never match any further **match** or **class** commands. If the first action is to log the packet, then a second action, such as dropping the packet, can occur. You can configure both the **drop-connection** and the **log** action for the same **match** or **class** command, in which case the packet is logged before it is dropped for a given match.

When you enable application inspection using the **inspect** command in a Layer 3/4 policy map (the **policy-map** command), you can enable the inspection policy map that contains this action, for example, enter the **inspect http** *http_policy_map* command where *http_policy_map* is the name of the inspection policy map.

Examples

The following example drops packets, closes the connection, and sends a log when they match the http-traffic class map. If the same packet also matches the second **match** command, it will not be processed because it was already dropped.

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

Related Commands

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

