



default through duplex Commands

default

To restore default settings for the **time-range** command **absolute** and **periodic** keywords, 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	<p>(Optional) 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.</p> <p>This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are:</p> <ul style="list-style-type: none"> daily—Monday through Sunday weekdays—Monday through Friday weekend—Saturday and Sunday <p>If the ending days of the week are the same as the starting days of the week, you can omit them.</p>
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

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
Time-range configuration	•	•	•	•	—

Command History

Release	Modification
7.0(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 security appliance; 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 security appliance based on time.

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
7.0(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	<p>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.</p> <p>This argument is any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. Other possible values are:</p> <ul style="list-style-type: none"> • daily—Monday through Sunday • weekdays—Monday through Friday • weekend—Saturday and Sunday <p>If the ending days of the week are the same as the starting days of the week, you can omit them.</p>
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
7.0(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 security appliance; 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 security appliance 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
7.0(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
hostname<ca-trustpoint>#
```

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.

To delete all default domain names, use the **no default-domain** 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 security appliance 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.

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	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

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 security appliance 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
7.0(1)	This command was introduced.
7.1(1)	The default-group-policy command in webvpn configuration mode was deprecated. The default-group-policy command in tunnel-group general-attributes mode replaces it.

Usage Guidelines

In Release 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

The default group policy DfltGrpPolicy comes with the initial configuration of the security appliance. 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-tunnel-general)# default-group-policy first-policy
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)# address-pool (inside) addrpool11 addrpool12 addrpool13
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)# authorization-server-group aaa-server78
```

```
hostname(config-tunnel-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 general-attributes	Specifies the general attributes for the named tunnel-group.

default-group-policy (webvpn)

To specify the name of the group policy to use when the WebVPN or e-mail proxy configuration does not specify a group policy, use the **default-group-policy** command. WebVPN, IMAP4S, POP3S, and SMTPS sessions require either a specified or a default group policy. For WebVPN, use this command in webvpn mode. For e-mail proxy, use this command in the applicable e-mail proxy mode. To remove the attribute from the configuration, use the **no** version of this command.

default-group-policy *groupname*

no default-group-policy

Syntax Description

groupname	Identifies the previously configured group policy to use as the default group policy. Use the group-policy command in configuration mode to configure a group policy.
-----------	--

Defaults

A default group policy, named *DfltGrpPolicy*, always exists on the security appliance. This **default-group-policy** command lets you substitute a group policy that you create as the default group policy for WebVPN and e-mail proxy sessions. An alternative is to edit the *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
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
Smtps	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated in webvpn configuration mode and moved to tunnel-group general-attributes configuration mode.

Usage Guidelines

In Release 7.1(1), if you enter this command in webvpn configuration mode, it is transformed to the same command in tunnel-group general-attributes mode.

You can edit, but not delete the system DefaultGroupPolicy. It has the following AVPs:

Attribute	Default Value
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn attributes:	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	mpme

Examples

The following example shows how to specify a default group policy called WebVPN7 for WebVPN:

```
hostname(config)# webvpn  
hostname(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

To set a default idle timeout value for WebVPN users, use the **default-idle-timeout** command in webvpn mode. To remove the default idle timeout value from the configuration and reset the default, use the **no** form of this command.

The default idle timeout prevents stale sessions.

default-idle-timeout *seconds*

no default-idle-timeout

Syntax Description

seconds	Specifies the number of seconds for the idle time out. The minimum is 60 seconds, maximum is 1 day (86400 seconds).
---------	---

Defaults

1800 seconds (30 minutes).

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
Webvpn	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The security appliance uses the value you set here if there is no idle timeout defined for a user, if the value is 0, or if the value does not fall into the valid range.

We recommend that you set this command to a short time period. This is because a browser set to disable cookies (or one that prompts for cookies and then denies them) can result in a user not connecting but nevertheless appearing in the sessions database. If the maximum number of connections permitted is set to one (**vpn-simultaneous-logins** command), the user cannot log back in because the database indicates that the maximum number of connections already exists. Setting a low idle timeout removes such phantom sessions quickly, and lets a user log in again.

Examples

The following example shows how to set the default idle timeout to 1200 seconds (20 minutes):

```
hostname(config)# webvpn
hostname(config-webvpn)# default-idle-timeout 1200
```

Related Commands

Command	Description
vpn-simultaneous-logins	Sets the maximum number of simultaneous VPN sessions permitted. Use in group-policy or username mode.

default-information originate (OSPF)

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: <ul style="list-style-type: none"> 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
Preexisting	This command was preexisting.

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	Displays the commands in the global router configuration.
router	

default-information originate (RIP)

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

default-information originate [**route-map** *name*]

no default-information originate [**route-map** *name*]

Syntax Description

route-map *name* (Optional) Name of the route map to apply. The routing process generates the default route if the route map is satisfied.

Defaults

This command is disabled by default.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was Introduced.

Usage Guidelines

The route map referenced in the **default-information originate** command cannot use an extended access list; it can use a standard access list.

Examples

The following example shows how generate a default route into RIP:

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# default-information originate
```

Related Commands

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

delete

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

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

Syntax Description

/noconfirm	(Optional) Specifies not to prompt for confirmation.
/recursive	(Optional) Deletes the specified file recursively in all subdirectories.
filename	Specifies the name of the file to delete.
flash:	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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

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-message (group-policy webvpn configuration mode)

To change the message delivered to a remote user who logs into WebVPN successfully, but has no VPN privileges, use the **deny-message value** command in tunnel-group webvpn configuration mode.

The **no deny-message value** command removes the string, so that the remote user does not receive a message.

The **no deny-message none** command removes the attribute from the tunnel group policy configuration. The policy inherits the attribute value.

deny-message value "string"

no deny-message value

no deny-message none

Syntax Description

<i>string</i>	Up to 491 alphanumeric characters, including special characters, spaces, and punctuation.
---------------	---

Defaults

The default deny message is: "Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information."

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 webvpn configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.
7.1(1)	This command moved from tunnel-group webvpn configuration mode to group-policy webvpn configuration mode.

Usage Guidelines

Before entering this command, you must enter the **group-policy name** attributes in global configuration mode, then the **webvpn** command. (This assumes you already have created the policy *name*.)

When typing the string in the **deny-message value** command, continue typing even if the command wraps.

The text appears on the remote user's browser upon login, independent of the tunnel policy used for the VPN session.

Examples

The first command in the following example creates an internal group policy named group2. The subsequent commands modify the deny message associated with that policy.

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK. However,
you have not been granted rights to use the VPN features. Contact your administrator for
more information."
hostname(config-group-webvpn)
```

Related Commands

Command	Description
clear configure group-policy	Removes all group-policy configuration.
group-policy	Creates a group policy.
group-policy attributes	Enters the group-policy attribute configuration mode.
show running-config group-policy [name]	Displays the running group policy configuration (for the policy named).
webvpn (group-policy or username configuration mode)	Enters group-policy webvpn configuration mode.

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** version of the command.

deny version *version*

deny version *version*

Syntax Description

<i>version</i>	Specifies the version of SNMP traffic that the security appliance 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
7.0(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

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-map configuration	•	•	•	•	—
Context configuration	•	•	—	—	•
Gtp-map configuration	•	•	•	•	—
Interface configuration	•	•	•	•	•
Object-group configuration	•	•	•	•	—
Policy-map configuration	•	•	•	•	—

Command History

Release	Modification
7.0(1)	This command was added to several new configuration modes.

Examples

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

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(config-context)# config-url flash://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.
gtp-map	Controls parameters for the GTP inspection engine.
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.

dhcp client route distance

To configure an administrative distance for routes learned through DHCP, use the **dhcp client route distance** command in interface configuration mode. To restore the default setting, use the **no** form of this command.

dhcp client route distance *distance*

no dhcp client route distance *distance*

Syntax Description

distance The administrative distance to apply to routes learned through DHCP. Valid values are from 1 to 255.

Defaults

Routes learned through DHCP are given an administrative distance of 1 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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **dhcp client route distance** command is checked only when a route is learned from DHCP. If the **dhcp client route distance** command is entered after a route is learned from DHCP, the administrative distance specified does not affect the existing learned route. Only routes learned after the command was entered have the specified administrative distance.

You must specify the **setroute** option on the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEthernet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
```

```
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route track	Associates routes learned through DHCP with a tracking entry object.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp client route track

To configure the DHCP client to associate added routes with a specified tracked object number, use the **dhcp client route track** command in interface configuration mode. To disable DHCP client route tracking, use the **no** form of this command.

dhcp client route track *number*

no dhcp client route track

Syntax Description

number The tracking entry object ID. Valid values are from 1 to 500.

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
Interface configuration	•	—	•	—	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The **dhcp client route track** command is checked only when a route is learned from DHCP. If the **dhcp client route track** command is entered after a route is learned from DHCP, the existing learned routes are not associated with a tracking object. Only routes learned after the command was entered are associated with the specified tracking object.

You must specify the **setroute** option on the **ip address dhcp** command to obtain routes through DHCP.

If DHCP is configured on multiple interfaces, you must use the **dhcp client route distance** command on each of the interfaces to indicate the priority of the installed routes.

Examples

The following example obtains the default route through DHCP on GigabitEthernet0/2. The route is tracked by tracking entry object 1. The SLA operation monitors the availability of the 10.1.1.1 gateway off of the outside interface. If the SLA operation fails, then the backup route obtained through DHCP on GigabitEthernet0/3 is used. The backup route is assigned an administrative distance of 254.

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
```

```
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

Related Commands

Command	Description
dhcp client route distance	Assigns an administrative distance to routes learned through DHCP.
ip address dhcp	Configures the specified interface with an IP address obtained through DHCP.
sla monitor	Defines an SLA monitoring operation.
track rtr	Creates a tracking entry to poll the SLA.

dhcp-client update dns

To configure the update parameters that the DHCP client passes to the DHCP server, use the **dhcp-client update dns** command in global configuration mode. To remove the parameters that the DHCP client passes to the DHCP server, use the **no** form of this command.

dhcp-client update dns [server {both | none}]

no dhcp-client update dns [server {both | none}]

Syntax Description

both	The client requests that the DHCP server update both the DNS A and PTR resource records.
none	The client requests that the DHCP server perform no DDNS updates.
server	Specifies the DHCP server to receive the client requests.

Defaults

By default, the security appliance requests that the DHCP server perform PTR RR updates only. The client does not send the FQDN option to the server.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

This command can also be entered in interface configuration mode, but it is not hyphenated. See **dhcp client update dns**. When entered in interface mode, the **dhcp client update dns** command overrides settings configured by this command in global configuration mode.

Examples

The following example configures the client to request that the DHCP server update neither the A and the PTR RRs:

```
hostname(config)# dhcp-client update dns server none
```

The following example configures the client to request that the server update both the A and PTR RRs:

```
hostname(config)# dhcp-client update dns server both
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp client update dns	
dhcpd update dns	Enables a DHCP server to perform DDNS updates.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

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*



Note

The size of the pool is limited to 32 addresses with a 10-user license and 128 addresses with a 50-user license on the Cisco ASA 5505. The unlimited user license on the Cisco ASA 5505 and all other security appliance platforms support 256 addresses.

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
Preexisting	This command was preexisting.

Usage Guidelines

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

The size of the address pool is limited to 256 addresses per pool on the security appliance. If the address pool range is larger than 253 addresses, the netmask of the security appliance 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 security appliance 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 dhcpcd address *interface_name*** command removes the DHCP server address pool that you configured for the specified interface.

Refer to the *Cisco Security Appliance Command Line Configuration Guide* for information on how to implement the DHCP server feature into the security appliance.

Examples

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

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

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

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

Related Commands

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

dhcpd auto_config

To enable the security appliance to automatically configure DNS, WINS and domain name values for the DHCP server based on the values obtained from an interface running a DHCP or PPPoE client, or from a vpn server, use the **dhcpd auto_config** command in global configuration mode. To discontinue the automatic configuration of DHCP parameters, use the **no** form of this command.

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

Syntax Description

<i>client_if_name</i>	Specifies the interface running the DHCP client that supplies the DNS, WINS, and domain name parameters.
interface <i>if_name</i>	Specifies the interface to which the action will apply.
vpnclient-wins-override	Overrides interface DHCP or PPPoE client WINS parameter with vpnclient parameter.

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
Preexisting	This command was preexisting.

Usage Guidelines

If you specify DNS, WINS, or domain name parameters using the CLI commands, then the CLI-configured parameters overwrite the parameters obtained by automatic configuration.

Examples

The following example shows how to configure DHCP on the inside interface. The **dhcpd auto_config** command is used to pass DNS, WINS, and domain information obtained from the DHCP client on the outside interface to the DHCP clients on the inside interface.

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd autoconfig outside
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 ip address dhcp server	Displays detailed information about the DHCP options provided by a DHCP server to an interface acting as a DHCP client.
	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*] [**interface** *if_name*]

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

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.
interface <i>if_name</i>	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

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 security appliance.

```
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* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

Syntax Description

<i>domain_name</i>	The DNS domain name, for example example.com.
interface <i>if_name</i>	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all 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
Global configuration	•	•	•	•	—

Command History

Release	Modification
Preexisting	This command was preexisting.

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 security appliance:

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

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
Preexisting	This command was preexisting.

Usage Guidelines

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 security appliance 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 security appliance DHCP server daemon does not support clients that are not directly connected to a security appliance interface.

Refer to the *Cisco Security Appliance Command Line Configuration Guide* for information on how to implement the DHCP server feature into the security appliance.

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* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

Syntax Description

interface <i>if_name</i>	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
<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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

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*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

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 with several exceptions. 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.
interface <i>if_name</i>	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

When a DHCP option request arrives at the security appliance DHCP server, the security appliance 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 RFC2132.

**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* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

Syntax Description

interface <i>if_name</i>	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
<i>number</i>	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:

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

The security appliance 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 security appliance 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 update dns

To enable a DHCP server to perform Dynamic DNS updates, use the **dhcpd update dns** command in global configuration mode. To disable DDNS by a DHCP server, use the **no** form of this command.

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

Syntax Description

both	Specifies that the DHCP server updates both A and PTR DNS resource records (RRs).
interface	Specifies the security appliance interface to which the DDNS updates apply.
override	Specifies that the DHCP server overrides DHCP client requests.
<i>srv_ifc_name</i>	Specifies an interface to apply this option to.

Defaults

By default, the DHCP server performs PTR RR updates only.

Command Modes

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

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

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

Dynamic DNS (DDNS) updates the name to address and address to name mappings maintained by DNS. Updates are performed in conjunction with a DHCP server. The **dhcpd update dns** command enables updates by the server.

Name and address mappings are contained in two types of resource records (RR):

- The A resource record contains domain name to IP address mappings.
- The PTR resource record contains IP address to domain name mappings.

DDNS updates can be used to maintain consistent information between the A and PTR RR types.

Using the **dhcpd update dns** command, the DHCP server can be configured to perform both A and PRT RR updates or PTR RR updates only. It can also be configured to override update requests from the DHCP client.

Examples

The following example configures the DDNS server to perform both A and PTR updates while also overriding requests from the DHCP client:

```
hostname(config)# dhcpcd update dns both override
```

Related Commands

Command	Description
ddns (DDNS-update-method mode)	Specifies a DDNS update method type for a created DDNS method.
ddns update (interface config mode)	Associates a dynamic DNS (DDNS) update method with a security appliance interface or a DDNS update hostname.
ddns update method (global config mode)	Creates a method for dynamically updating DNS resource records.
dhcp-client update dns	Configures the update parameters that the DHCP client passes to the DHCP server.
interval maximum	Configures the maximum interval between update attempts by a DDNS update method.

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*] [**interface** *if_name*]

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

Syntax Description

interface <i>if_name</i>	Specifies the interface to which values entered to the server apply. If no interface is specified, values are applied to all servers.
<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
Preexisting	This command was preexisting.

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.

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 security appliance 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
Preexisting	This command was preexisting.

Usage Guidelines

For the security appliance 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 security appliance 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 security appliance, client requests on the inside interface of the security appliance, 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 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 security appliance 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 security appliance 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
Preexisting	This command was preexisting.

Usage Guidelines

You can add up to four DHCP relay servers per interface. You must add at least one **dhcprelay server** command to the security appliance 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.

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 security appliance, client requests on the inside interface of the security appliance, 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 security appliance 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 <i>interface</i> .
--------------------	-----------	---

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
	Preexisting	This command was preexisting.

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 security appliance adds one containing the address of *interface*. This action allows the client to set its default route to point to the security appliance.

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

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 security appliance:

```
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
Preexisting	This command was preexisting.

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 security appliance, client requests on the inside interface of the security appliance, 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.

dialog

To customize dialog messages displayed to WebVPN users, use the **dialog** command from webvpn customization mode:

dialog { **title** | **message** | **border** } **style** *value*

[**no**] **dialog** { **title** | **message** | **border** } **style** *value*

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

Syntax Description

title	Specifies you are changing the title.
message	Specifies you are changing the message.
border	Specifies you are changing the border.
style	Specifies you are changing the style.
<i>value</i>	The actual text to display (maximum 256 characters), or Cascading Style Sheet (CSS) parameters (maximum 256 characters).

Defaults

The default title style is background-color:#669999;color:white.

The default message style is background-color:#99CCCC;color:black.

The default border style is border:1px solid black;border-collapse:collapse.

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
Webvpn customization	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

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

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

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

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

**Note**

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

Examples

The following example customizes the dialog message, changing the foreground color to blue:

```
F1-asal(config)# webvpn
F1-asal(config-webvpn)# customization cisco
F1-asal(config-webvpn-custom)# dialog message style color:blue
```

Related Commands

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

dir

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

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

Syntax Description		
/all	(Optional)	Displays all files.
all-fileSYSTEMS	(Optional)	Displays the files of all fileSYSTEMS
/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
	7.0(1)	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
Preexisting	This command was preexisting.

Usage Guidelines Use the **enable** command to enter privileged mode. The **disable** command allows you to exit privileged mode and returns you to unprivileged mode.

Examples The following example shows how to enter privileged mode:

```
hostname> enable
hostname#
```

The following example shows how to exit privileged mode:

```
hostname# disable
hostname>
```

Command	Description
enable	Enables privileged EXEC mode.

disable (cache)

To disable caching for WebVPN, use the **disable** command in cache mode. To reenable caching, use the **no** version of the command

disable

no disable

Defaults

Caching is enabled with default settings for each cache attribute.

Command Modes

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

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

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

Caching stores frequently reused objects in the system cache, which reduces the need to perform repeated rewriting and compressing of content. It reduces traffic between WebVPN and both the remote servers and end-user browsers, with the result that many applications run much more efficiently.

Examples

The following example shows how to disable caching, and how to then reenable it.

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# disable
hostname(config-webvpn-cache)# no disable
hostname(config-webvpn-cache)#
```

Related Commands

Command	Description
cache	Enters WebVPN Cache mode.
cache-compressed	Configures WebVPN cache compression.
expiry-time	Configures the expiration time for caching objects without revalidating them.
lmfactor	Sets a revalidation policy for caching objects that have only the last-modified timestamp.

■ disable (cache)

Command	Description
max-object-size	Defines the maximum size of an object to cache.
min-object-size	Defines the minimum size of an object to cache.

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
Preexisting	This command was preexisting.

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 re-enter 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 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:

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

Command History

Release	Modification
7.2(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 limits filters routing updates on the outside interface. It accepts routes in the 10.0.0.0 network and denies all others.

```
hostname(config)# access-list ripfilter permit 10.0.0.0
hostname(config)# access-list ripfilter deny any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter in interface outside
```

Related Commands

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

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

distribute-list out

To filter specific networks from being sent in RIP 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* | **rip** | **ospf** *pid* | **static** | **connected**]

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

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.
rip	(Optional) Filters only RIP routes.
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
7.2(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example prevents the 10.0.0.0 network from being advertised in RIP updates sent out of any interface.

```
hostname(config)# access-list ripfilter deny 10.0.0.0
hostname(config)# access-list ripfilter permit any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter out
```

Related Commands	Command	Description
	distribute-list in	Filters networks received in RIP updates.
	router rip	Enters router configuration mode.
	show running-config router	Displays the commands in the global router configuration.

dns domain-lookup

To enable the security appliance 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 security appliance 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
7.0(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 security appliance 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 security appliance caches information returned from external DNS requests. The security appliance 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 security appliance 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-group (tunnel-group webvpn configuration mode)

To specify the DNS server to use for a WebVPN tunnel-group, use the **dns-group** command in tunnel-group webvpn configuration mode. To restore the default DNS group, use the **no** form of this command.

dns-group *name*

no dns-group

Syntax Description

<i>name</i>	Specifies the name of the DNS server group configuration to use for the tunnel group.
-------------	---

Defaults

The default value is DefaultDNS.

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 webvpn-attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.1(1)	This command was introduced.

Usage Guidelines

The name can specify any DNS group. The dns-group command resolves the hostname to the appropriate DNS server for the tunnel group.

You configure the DNS group using the **dns server-group** command.

Examples

The following example shows a customization command that specifies the use of the DNS group named “dnsgroup1”:

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group dnsgroup1
hostname(config-tunnel-webvpn)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
dns server-group	Enters DNS-server-group mode, in which you can configure a DNS server group.
show running-config dns-server group	Shows one or all the existing DNS server-group configurations.
tunnel-group webvpn-attributes	Enters the config-webvpn mode for configuring WebVPN tunnel-group attributes.

dns-guard

To enable the DNS guard function, which enforces one DNS response per query, use the **dns-guard** command in parameters configuration mode. To disable this feature, use the **no** form of this command.

dns-guard

no dns-guard

Syntax Description

This command has no arguments or keywords.

Defaults

DNS guard is enabled by default. This feature can be enabled when **inspect dns** is configured even if a **policy-map type inspect dns** is not defined. To disable, **no dns-guard** must explicitly be stated in the policy map configuration. If **inspect dns** is not configured, the behavior is determined by the **global dns-guard** 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
Parameters configuration	•	•	•	•	—

Command History

Release	Modification
7.2(1)	This command was introduced.

Usage Guidelines

The identification field in the DNS header is used to match the DNS response with the DNS header. One response per query is allowed through the security appliance.

Examples

The following example shows how to enable DNS guard in a DNS inspection policy map:

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
```

Related Commands

Command	Description
class	Identifies a class map name in the policy map.
class-map type inspect	Creates an inspection class map to match traffic specific to an application.

Command	Description
policy-map	Creates a Layer 3/4 policy map.
show running-config policy-map	Display all current policy map configurations.

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. The security appliance uses DNS to resolve server names in your WebVPN configuration or certificate configuration (see “[Usage Guidelines](#)” for a list of supported commands). 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.

dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

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

Syntax Description

<i>ip_address</i>	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 security appliance saves each server in a separate command in the configuration. The security appliance 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
7.0(1)	This command was introduced.
7.1(1)	This command is deprecated. The name-server command in dns-server-group configuration mode replaces it.

Usage Guidelines

To enable DNS lookup, configure the **domain-name** command in dns-server-group configuration mode. If you do not enable DNS lookup, the DNS servers are not used.

WebVPN commands that support DNS resolution include the following:

- **server (pop3s)**
- **server (imap4s)**
- **server (smtps)**
- **port-forward**

- **url-list**

Certificate 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 **retries** command to set how many times the security appliance tries the list of DNS servers.

Examples

The following example adds three DNS servers:

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

The security appliance saves the configuration as separate commands, as follows:

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

To add two additional servers, you can enter them as one command:

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

Or you can enter them as two commands:

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

To delete multiple servers you can enter them as multiple commands or as one command, as follows:

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

Related Commands

Command	Description
domain-name (dns-server-group configuration mode)	Enables the security appliance to perform a name lookup.
name-server (dns-server-group configuration mode)	Replaces the dns name-server command. Identifies one or more DNS name servers.
retries (dns-server-group configuration mode)	Specifies the number of times to retry the list of DNS servers when the security appliance does not receive a response.
timeout (dns-server-group configuration mode)	Specifies the amount of time to wait before trying the next DNS server.

dns retries

To specify the number of times to retry the list of DNS servers when the security appliance 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
7.0(1)	This command was introduced.
7.1(1)	This command was deprecated for WebVPN connections.

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
dns domain-lookup	Enables the security appliance 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.

Command	Description
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

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	•	—	•	—	—

Command History

Release	Modification
7.0(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
```

dns server-group

To enter the dns server-group mode, in which you can specify the domain-name, name-server, number of retries, and timeout values for a DNS server to use for a tunnel-group, use the **dns server-group** command in global configuration mode. To remove a particular DNS server group, use the **no** form of this command.

dns server-group *name*

no dns server-group

Syntax Description

<i>name</i>	Specifies the name of the DNS server group configuration to use for the tunnel group.
-------------	---

Defaults

The default value is DefaultDNS.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The name can specify any DNS group. You configure the DNS group using the **dns server-group** command.

Examples

The following example configures a DNS server group named “eval”:

```
hostname(config)# dns server-group eval
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 192.168.10.10
hostname(config-dns-server-group)# retries 5
hostname(config-dns-server-group)# timeout 7
hostname(config-dns-server-group)#
```

Related Commands

Command	Description
clear configure dns	Removes all DNS commands.
show running-config dns server-group	Shows the current running DNS server-group configuration.

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 security appliance 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:

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

Command History

Release	Modification
7.0(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 security appliance does not receive a response.
dns domain-lookup	Enables the security appliance to perform a name lookup.
domain-name	Sets the default domain name.
show dns-hosts	Shows the DNS cache.

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. The security appliance 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.”

domain-name *name*

no domain-name [*name*]

Syntax Description

<i>name</i>	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
Preexisting	This command was preexisting.

Usage Guidelines

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 security appliance to perform a name lookup.
dns name-server	Configures a DNS server address.

■ domain-name

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

downgrade

To downgrade to a previous version of the operating system software (software image), use the **downgrade** command in privileged EXEC mode.



Caution

Do not load a previous version of software if your PIX security appliance is currently running PIX Version 7.0 or later. Loading a software image from monitor mode, on a PIX security appliance that has a PIX Version 7.0 file system, results in unpredictable behavior and is not supported. We strongly recommend that you use the **downgrade** command from a running PIX Version 7.0 image that facilitates the downgrade process.

downgrade *image_url* [**activation-key** [**flash** | *4-part_key* | *file*]] [**config** *start_config_url*]

Syntax Description

<i>4-part_key</i>	(Optional) Specifies the four-part activation key to write to the image. If you are using a five-part key, a warning with the list of features that might be lost by going back to the four-part key is generated. If the system Flash has been reformatted or erased, no default key is available for the downgrade. In that case, the CLI prompts you to enter an activation key at the command line. This is the default behavior if the activation-key keyword is not specified at the command line.
activation-key	(Optional) Specifies the activation key to use with the downgraded software image.
config	(Optional) Specifies the startup configuration file.
<i>file</i>	(Optional) Specifies the path/URL and name of the activation key file to use after the downgrade procedure completes. If the source image file is the one saved in Flash during the upgrade process, the activation key in this file is used with the downgrade.
flash	(Optional) Specifies to look in Flash memory for the four-part activation key that was used on the device prior to using a five-part activation key. This is the default behavior if the activation-key keyword is not specified at the command line.
<i>image_url</i>	Specifies the path/URL and name of the software image to downgrade to. The software image must be a version prior to 7.0(1).
<i>start_config_url</i>	(Optional) Specifies the path/URL and name of the configuration file to use after the downgrade procedure completes.

Defaults

If the **activation-key** keyword is not specified, the security appliance tries to use the last four-part activation key used. If the security appliance cannot find a four-part activation key in Flash, the command is rejected and an error message displays. In this case, a valid four-part activation-key must be specified at the command line next time. The default activation key or the user specified activation key is compared with the activation key currently in effect. If there is a potential loss of features by using the chosen activation key, a warning displays with the list of features that could be lost after downgrade.

The security appliance uses downgrade.cfg by default if the startup configuration file is not specified.

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
7.0(1)	This command was introduced.

Usage Guidelines

This command is available only on Cisco PIX Firewall series security appliances running software Release 7.0(1) and later. This command is not supported on Cisco ASA 5500 series security appliances.

**Caution**

A power failure during the downgrade process might corrupt the Flash memory. As a precaution, backup all data on the Flash memory to an external device prior to starting the downgrade process.

Recovering corrupt Flash memory requires direct console access. See the **format** command for more information.

Examples

The following example downgrades the software to Release 6.3.3:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
32c261f3 062afe24 c94ef2ea 0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded
```

Rebooting....

Enter zero actkey:

The following example shows what happens if you enter an invalid activation key:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
0 0 0 0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
Error: activation key entered is invalid.

Enter the file option when there is no actkey in the source image (happens if the source
is in tftp server).
```

The following example shows what happens if you specify the activation key in the source image and it does not exist:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key file
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
Activation key does not exist in the source image.
Please use the activation-key option to specify an activation key.
```

The following example shows how to abort the downgrade procedure at the final prompt:

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm] ===<typed n here>
Downgrade process terminated.
```

To downgrade, the software version must be less than 7.0. The following example shows a failed attempt at downgrading the software:

```
hostname# downgrade tftp://17.13.2.25//scratch/views/test/target/sw/cdisk
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Error: Need to use an image with version less than 7-0-0-0.

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

```
hostname# downgrade tftp://17.13.2.25//tftboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
VPN-3DES-AES
GTP/GPRS
5 Security Contexts
Failover is different:
current activation key in flash: UR(estricted)
4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

11-94

drop

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. To disable this action, use the **no** form of this command.

drop [send-protocol-error] [log]

no drop [send-protocol-error] [log]

Syntax Description

send-protocol-error	Sends a protocol error message.
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
7.2(1)	This command was introduced.

Usage Guidelines

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-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. The connection will be removed from the connection database on the security appliance. Any subsequent packets entering the security appliance for the dropped connection will be discarded. This drop-connection action is available in an inspection policy map (the **policy-map type inspect** command) for application traffic; however, not all applications allow this action. To disable this action, use the **no** form of this command.

drop-connection [send-protocol-error] [log]

no drop-connection [send-protocol-error] [log]

Syntax Description

send-protocol-error	Sends a protocol error message.
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
7.2(1)	This command was introduced.

Usage Guidelines

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.

duplex

To set the duplex of a copper (RJ-45) Ethernet interface, use the **duplex** command in interface configuration mode. To restore the duplex setting to the default, use the **no** form of this command.

duplex { auto | full | half }

no duplex

Syntax Description

auto	Auto-detects the duplex mode.
full	Sets the duplex mode to full duplex.
half	Sets the duplex mode to half duplex.

Defaults

The default is auto detect.

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

Usage Guidelines

Set the duplex mode on the physical interface only.

The **duplex** command is not available for fiber media.

If your network does not support auto detection, set the duplex mode to a specific value.

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

If you set the duplex to anything other than **auto** on PoE ports, if available, then Cisco IP phones and Cisco wireless access points that do not support IEEE 802.3af will not be detected and supplied with power.

Examples

The following example sets the duplex mode to full duplex:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

Related Commands

Command	Description
clear configure interface	Clears all configuration for an interface.
interface	Configures an interface and enters interface configuration mode.
show interface	Displays the runtime status and statistics of interfaces.
show running-config interface	Shows the interface configuration.
speed	Sets the interface speed.

