CHAPTER 16

interface-dhcp through issuer-name Commands

intercept-dhcp

To enable DHCP Intercept, use the **intercept-dhcp enable** command in group-policy configuration mode. To disable DHCP Intercept, use the **intercept-dhcp disable** command.

To remove the intercept-dhcp attribute from the running configuration, use the **no intercept-dhcp** command. This lets users inherit a DHCP Intercept configuration from the default or other group policy.

DHCP Intercept lets Microsoft XP clients use split-tunneling with the security appliance. The security appliance replies directly to the Microsoft Windows XP client DHCP Inform message, providing that client with the subnet mask, domain name, and classless static routes for the tunnel IP address. For Windows clients prior to XP, DHCP Intercept provides the domain name and subnet mask. This is useful in environments in which using a DHCP server is not advantageous

intercept-dhcp *netmask* {**enable | disable**}

no intercept-dhcp

Syntax Description

disable	Disables DHCP Intercept.
enable	Enables DHCP Intercept.
netmask	Provides the subnet mask for the tunnel IP address.

Defaults

DHCP Intercept is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

A Microsoft XP anomaly results in the corruption of domain names if split tunnel options exceed 255 bytes. To avoid this problem, the security appliance limits the number of routes it sends to 27 to 40 routes, with the number of routes dependent on the classes of the routes.

Examples

The following example shows how to set DHCP Intercept S for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

interface

To configure an interface and enter interface configuration mode, use the **interface** command in global configuration mode. To create a logical subinterface, use the **.***subinterface* argument. To remove a subinterface, use the **no** form of this command; you cannot remove a physical interface. In interface configuration mode, you can configure hardware settings, assign a name, assign a VLAN, assign an IP address, and configure many other settings.

interface {*physical_interface*[**.***subinterface*] | *mapped_name*}

no interface *physical_interface***.***subinterface*

Syntax Description

mapped_name	In multiple context mode, enter the mapped name if it was assigned using the **allocate-interface** command.
physical_interface	The physical interface type, slot, and port number as *type*[*slot*/]*port*. A space between the type and slot/port is optional. The physical interface types include the following: • **ethernet** • **gigabitethernet** For the PIX 500 series security appliance, enter the type followed by the port number, for example, **ethernet0**. For the ASA 5500 series adaptive security appliance, enter the type followed by slot/port, for example, **gigabitethernet0/1**. Interfaces that are built into the chassis are assigned to slot 0, while interfaces on the 4GE SSM are assigned to slot 1. The ASA 5500 series adaptive security appliance also includes the following type: • **management** The management interface is a Fast Ethernet interface designed for management traffic only, and is specified as **management0/0**. You can, however, use it for through traffic if desired (see the **management-only** command). In transparent firewall mode, you can use the management interface in addition to the two interfaces allowed for through traffic. You can also add subinterfaces to the management interface to provide management in each security context for multiple context mode. See the hardware documentation that came with your model to identify the interface type, slot, and port number.
subinterface	(Optional) An integer between 1 and 4294967293 designating a logical subinterface. The maximum number of subinterfaces varies depending on your security appliance model. See the *Cisco Security Appliance Command Line Configuration Guide* for the maximum subinterfaces per platform.

Defaults

By default, the security appliance automatically generates **interface** commands for all physical interfaces.

In multiple context mode, the security appliance automatically generates **interface** commands for all interfaces allocated to the context using the **allocate-interface** command.

All physical interfaces are shut down by default. Allocated interfaces in contexts are not shut down in the configuration.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was modified to allow for new subinterface naming conventions and to change arguments to be separate commands under interface configuration mode.

Usage Guidelines

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through an enabled subinterface. For multiple context mode, if you allocate a physical interface or subinterface to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must also enable the interface in the system configuration. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For subinterfaces, configure the **vlan** command. The security level is 0 (lowest) by default. See the **security-level** command for default levels for some interfaces or to change from the default of 0 so interfaces can communicate with each other.

The ASA adaptive security appliance includes a dedicated management interface called Management 0/0, which is meant to support traffic to the security appliance. However, you can configure any interface to be a management-only interface using the **management-only** command. Also, for Management 0/0, you can disable management-only mode so the interface can pass through traffic just like any other interface.

Note Transparent firewall mode allows only two interfaces to pass through traffic; however, on the ASA adaptive security appliance, you can use the dedicated management interface (either the physical interface or a subinterface) as a third interface for management traffic. The mode is not configurable in this case and must always be management-only.

If you change interface settings, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

You cannot delete the physical interfaces using the **no** form of the **interface** command, nor can you delete the allocated interfaces within a context.

In multiple context mode, you configure physical parameters, subinterfaces, and VLAN assignments in the system configuration only. You configure other parameters in the context configuration only.

Examples

The following example configures parameters for the physical interface in single mode:

```
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
```

The following example configures parameters for a subinterface in single mode:

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

The following example configures interface parameters in multiple context mode for the system configuration, and allocates the gigabitethernet 0/1.1 subinterface to contextA:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

The following example configures parameters in multiple context mode for the context configuration:

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

Related Commands

Command	Description
allocate-interface	Assigns interfaces and subinterfaces to a security context.
clear configure interface	Clears all configuration for an interface.
clear interface	Clears counters for the **show interface** command.
show interface	Displays the runtime status and statistics of interfaces.

interface (vpn load-balancing)

To specify a non-default public or private interface for VPN load-balancing in the VPN load-balancing virtual cluster, use the **interface** command in vpn load-balancing mode. To remove the interface specification and revert to thte default interface, use the **no** form of this command.

interface {**lbprivate** | **lbpublic**} *interface-name*]

no interface {**lbprivate** | **lbpublic**}

Syntax Description

interface-name	The name of the interface to be configured as the public or private interface for the VPN load-balancing cluster.
lbprivate	Specifies that this command configures the private interface for VPN load-balancing.
lbpublic	Specifies that this command configures the public interface for VPN load-balancing.

Defaults

If you omit the **interface** command, the **lbprivate** interface defaults to **inside**, and the **lbpublic** interface defaults to **outside**.

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
vpn load-balancing	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must have first used the **vpn load-balancing** command to enter vpn load-balancing mode.

You must also have previously used the **interface**, **ip address** and **nameif** commands to configure and assign a name to the interface that you are specifying in this command.

The no form of this command reverts the interface to its default.

Examples

The following is an example of a **vpn load-balancing** command sequence that includes an **interface** command that specifies the public interface of the cluster as “test” one that reverts the private interface of the cluster to the default (inside):

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
```

```
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# no interface lbprivate
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

Related Commands

Command	Description
vpn load-balancing	Enter VPN load-balancing mode.

interface-policy

To specify the policy for failover when monitoring detects an interface failure, use the **interface-policy** command in failover group configuration mode. To restore the default values, use the **no** form of this command.

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

Syntax Description

num	Specifies a number from 1 to 100 when used as a percentage, or 1 to the maximum number of interfaces.
%	(Optional) Specifies that the number *num* is a percentage of the monitored interfaces.

Defaults

If the **failover interface-policy** command is configured for the unit, then the default for the **interface-policy** failover group command assumes that value. If not, then *num* is 1.

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
Failover group configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

There is no space between the *num* argument and the optional **%** keyword.

If the number of failed interfaces meets the configured policy and the other security appliance is functioning properly, the security appliance will mark itself as failed and a failover may occur (if the active security appliance is the one that fails). Only interfaces that are designated as monitored by the **monitor-interface** command count towards the policy.

Examples

The following partial example shows a possible configuration for a failover group:

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
hostname(config)#
```

Related Commands

Command	Description
failover group	Defines a failover group for Active/Active failover.
failover interface-policy	Configures the interface monitoring policy.
monitor-interface	Specifies the interfaces being monitored for failover.

ip-address

To include the security appliance IP address in the certificate during enrollment, use the **ip-addr** command in crypto ca trustpoint configuration mode. To restore the default setting, use the **no** form of the command.

ip-address *ip-address*

no ip-address

Syntax Description

ip-address	Specifies the IP address of the security appliance.

Defaults

The default setting is to not include the IP address.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the security appliance IP address in the enrollment request for trustpoint central:

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# ip-address 209.165.200.225
```

Related Commands

Command	Description
crypto ca trustpoint	Enters trustpoint configuration mode.
default enrollment	Returns enrollment parameters to their defaults.

ip address

To set the IP address for an interface (in routed mode) or for the management address (transparent mode), use the **ip address** command. For routed mode, enter this command in interface configuration mode. In transparent mode, enter this command in global configuration mode. To remove the IP address, use the **no** form of this command. This command also sets the standby address for failover.

ip address *ip_address* [*mask*] [**standby** *ip_address*]

no ip address [*ip_address*]

Syntax Description

ip_address	The IP address for the interface (routed mode) or the management IP address (transparent mode).
mask	(Optional) The subnet mask for the IP address. If you do not set the mask, the security appliance uses the default mask for the IP address class.
standby *ip_address*	(Optional) The IP address for the standby unit for failover.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.

Usage Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

A transparent firewall does not participate in IP routing. The only IP configuration required for the security appliance is to set the management IP address. This address is required because the security appliance uses this address as the source address for traffic originating on the security appliance, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context.

The standby IP address must be on the same subnet as the main IP address.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```

The following example sets the management address and standby address of a transparent firewall:

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address dhcp	Sets the interface to obtain an IP address from a DHCP server.
show ip address	Shows the IP address assigned to an interface.

ip address dhcp

To use DHCP to obtain an IP address for an interface, use the **ip address dhcp** command in interface configuration mode. To disable the DHCP client for this interface, use the **no** form of this command.

ip address dhcp [**setroute**]

no ip address dhcp

Syntax Description

setroute	(Optional) Allows the security appliance to use the default route supplied by the DHCP server.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was changed from a global configuration command to an interface configuration mode command. You can also enable this command on any interface, instead of only the outside interface.

Usage Guidelines

Reenter this command to reset the DHCP lease and request a new lease.

You cannot set this command at the same time as the **ip address** command.

If you enable the **setroute** option, do not configure a default route using the **route** command.

If you do not enable the interface using the **no shutdown** command before you enter the **ip address dhcp** command, some DHCP requests might not be sent.

Examples

The following example enables DHCP on the gigabitethernet0/1 interface:

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown
hostname(config-if)# ip address dhcp
```

Related Commands

Command	Description
interface	Configures an interface and enters interface configuration mode.
ip address	Sets the IP address for the interface or sets the management IP address for a transparent firewall.
show ip address dhcp	Shows the IP address obtained from the DHCP server.

ip audit attack

To set the default actions for packets that match an attack signature, use the **ip audit attack** command in global configuration mode. To restore the default action (to reset the connection), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, the security appliance assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Defaults

The default action is to send and alarm.

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

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an attack signature. The audit policy for the inside interface overrides this default to be alarm only, while the policy for the outside interface uses the default setting set with the **ip audit attack** command.

```
hostname(config)# ip audit attack action alarm reset
```

```
hostname(config)# ip audit name insidepolicy attack action alarm
hostname(config)# ip audit name outsidepolicy attack
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
show running-config ip audit attack	Shows the configuration for the **ip audit attack** command.

ip audit info

To set the default actions for packets that match an informational signature, use the **ip audit info** command in global configuration mode. To restore the default action (to generate an alarm), use the **no** form of this command. You can specify multiple actions, or no actions.

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

Syntax Description

action	(Optional) Specifies that you are defining a set of default actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, the security appliance assumes you entered it, and the **action** keyword appears in the configuration.
alarm	(Default) Generates a system message showing that a packet matched a signature.
drop	(Optional) Drops the packet.
reset	(Optional) Drops the packet and closes the connection.

Defaults

The default action is to generate an alarm.

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

You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

For a list of signatures, see the **ip audit signature** command.

Examples

The following example sets the default action to alarm and reset for packets that match an informational signature. The audit policy for the inside interface overrides this default to be alarm and drop, while the policy for the outside interface uses the default setting set with the **ip audit info** command.

```
hostname(config)# ip audit info action alarm reset
```

```
hostname(config)# ip audit name insidepolicy info action alarm drop
hostname(config)# ip audit name outsidepolicy info
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

Related Commands

Command	Description
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
show running-config ip audit info	Shows the configuration for the **ip audit info** command.

ip audit interface

To assign an audit policy to an interface, use the **ip audit interface** command in global configuration mode. To remove the policy from the interface, use the **no** form of this command.

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

Syntax Description

interface_name	Specifies the interface name.
policy_name	The name of the policy you added with the **ip audit name** command. You can assign an **info** policy and an **attack** policy to each interface.

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.

Examples

The following example applies audit policies to the inside and outside interfaces:

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.

Command	Description
ip audit signature	Disables a signature.
show running-config ip audit interface	Shows the configuration for the **ip audit interface** command.

ip audit name

To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use the **ip audit name** command in global configuration mode. Signatures are activities that match known attack patterns. For example, there are signatures that match DoS attacks. To remove the policy, use the **no** form of this command.

ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {**info** | **attack**} [**action** [**alarm**] [**drop**] [**reset**]]

Syntax Description

action	(Optional) Specifies that you are defining a set of actions. If you do not follow this keyword with any actions, then the security appliance takes no action. If you do not enter the **action** keyword, then the security appliance uses the default action set by the **ip audit attack** and **ip audit info** commands.
alarm	(Optional) Generates a system message showing that a packet matched a signature.
attack	Creates an audit policy for attack signatures; the packet might be part of an attack on your network, such as a DoS attack or illegal FTP commands.
drop	(Optional) Drops the packet.
info	Creates an audit policy for informational signatures; the packet is not currently attacking your network, but could be part of an information-gathering activity, such as a port sweep.
name	Sets the name of the policy.
reset	(Optional) Drops the packet and closes the connection.

Defaults

If you do not change the default actions using the **ip audit attack** and **ip audit info** commands, then the default action for attack signatures and informational signatures is to generate an alarm.

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

To apply the policy, assign it to an interface using the **ip audit interface** command. You can assign an **info** policy and an **attack** policy to each interface.

For a list of signatures, see the **ip audit signature** command.

If traffic matches a signature, and you want to take action against that traffic, use the **shun** command to prevent new connections from the offending host and to disallow packets from any existing connection.

Examples

The following example sets an audit policy for the inside interface to generate an alarm for attack and informational signatures, while the policy for the outside interface resets the connection for attacks:

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit signature	Disables a signature.
shun	Blocks packets with a specific source and destination address.

ip audit signature

To disable a signature for an audit policy, use the **ip audit signature** command in global configuration mode. To reenable the signature, use the **no** form of this command. You might want to disable a signature if legitimate traffic continually matches a signature, and you are willing to risk disabling the signature to avoid large numbers of alarms.

ip audit signature *signature_number* **disable**

no ip audit signature *signature_number*

Syntax Description

signature_number	Specifies the signature number to disable. See Table 16-1 for a list of supported signatures.
disable	Disables the signature.

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

Table 16-1 lists supported signatures and system message numbers.

Table 16-1 Signature IDs and System Message Numbers

Signature ID	Message Number	Signature Title	Signature Type	Description
1000	400000	IP options-Bad Option List	Informational	Triggers on receipt of an IP datagram where the list of IP options in the IP datagram header is incomplete or malformed. The IP options list contains one or more options that perform various network management or debugging tasks.
1001	400001	IP options-Record Packet Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
1002	400002	IP options-Timestamp	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).
1003	400003	IP options-Security	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).
1004	400004	IP options-Loose Source Route	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).
1005	400005	IP options-SATNET ID	Informational	Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).
1006	400006	IP options-Strict Source Route	Informational	Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).
1100	400007	IP Fragment Attack	Attack	Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field.
1102	400008	IP Impossible Packet	Attack	Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.
1103	400009	IP Overlapping Fragments (Teardrop)	Attack	Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS.
2000	400010	ICMP Echo Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply).
2001	400011	ICMP Host Unreachable	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable).

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
2002	400012	ICMP Source Quench	Informational	Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench).
2003	400013	ICMP Redirect	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect).
2004	400014	ICMP Echo Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request).
2005	400015	ICMP Time Exceeded for a Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram).
2006	400016	ICMP Parameter Problem on Datagram	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram).
2007	400017	ICMP Timestamp Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request).
2008	400018	ICMP Timestamp Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply).
2009	400019	ICMP Information Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request).
2010	400020	ICMP Information Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply).
2011	400021	ICMP Address Mask Request	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request).
2012	400022	ICMP Address Mask Reply	Informational	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply).

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
2150	400023	Fragmented ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field.
2151	400024	Large ICMP Traffic	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024.
2154	400025	Ping of Death Attack	Attack	Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and (IP offset * 8) + (IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet.
3040	400026	TCP NULL flags	Attack	Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host.
3041	400027	TCP SYN+FIN flags	Attack	Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host.
3042	400028	TCP FIN only flags	Attack	Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host.
3153	400029	FTP Improper Address Specified	Informational	Triggers if a port command is issued with an address that is not the same as the requesting host.
3154	400030	FTP Improper Port Specified	Informational	Triggers if a port command is issued with a data port specified that is <1024 or >65535.
4050	400031	UDP Bomb attack	Attack	Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt.
4051	400032	UDP Snork attack	Attack	Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected.
4052	400033	UDP Chargen DoS attack	Attack	This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19.
6050	400034	DNS HINFO Request	Informational	Triggers on an attempt to access HINFO records from a DNS server.

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
6051	400035	DNS Zone Transfer	Informational	Triggers on normal DNS zone transfers, in which the source port is 53.
6052	400036	DNS Zone Transfer from High Port	Informational	Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53.
6053	400037	DNS Request for All Records	Attack	Triggers on a DNS request for all records.
6100	400038	RPC Port Registration	Informational	Triggers when attempts are made to register new RPC services on a target host.
6101	400039	RPC Port Unregistration	Informational	Triggers when attempts are made to unregister existing RPC services on a target host.
6102	400040	RPC Dump	Informational	Triggers when an RPC dump request is issued to a target host.
6103	400041	Proxied RPC Request	Attack	Triggers when a proxied RPC request is sent to the portmapper of a target host.
6150	400042	ypserv (YP server daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.
6151	400043	ypbind (YP bind daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.
6152	400044	yppasswdd (YP password daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.
6153	400045	ypupdated (YP update daemon) Portmap Request	Attack	Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	Attack	Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.
6155	400047	mountd (mount daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the mount daemon (mountd) port.
6175	400048	rexd (remote execution daemon) Portmap Request	Informational	Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port.

Table 16-1 Signature IDs and System Message Numbers (continued)

Signature ID	Message Number	Signature Title	Signature Type	Description
6180	400049	rexd (remote execution daemon) Attempt	Informational	Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources.
6190	400050	statd Buffer Overflow	Attack	Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

Examples

The following example disables signature 6100:

```
hostname(config)# ip audit signature 6100 disable
```

Related Commands

Command	Description
ip audit attack	Sets the default actions for packets that match an attack signature.
ip audit info	Sets the default actions for packets that match an informational signature.
ip audit interface	Assigns an audit policy to an interface.
ip audit name	Creates a named audit policy that identifies the actions to take when a packet matches an attack signature or an informational signature.
show running-config ip audit signature	Shows the configuration for the **ip audit signature** command.

ip-comp

To enable LZS IP compression, use the **ip-comp enable** command in group-policy configuration mode. To disable IP compression, use the **ip-comp disable** command.

To remove the **ip-comp** attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value from another group policy.

ip-comp {**enable | disable**}

no ip-comp

Syntax Description

disable	Disables IP compression.
enable	Enables IP compression.

Defaults

IP compression is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Enabling data compression might speed up data transmission rates for remote dial-in users connecting with modems.

Caution Data compression increases the memory requirement and CPU utilization for each user session and consequently decreases the overall throughput of the security appliance. For this reason, we recommend that you enable data compression only for remote users connecting with a modem. Design a group policy specific to modem users, and enable compression only for them.

Examples

The following example shows how to enable IP compression for the group policy named “FirstGroup”:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-comp enable
```

ip local pool

To configure IP address pools to be used for VPN remote access tunnels, use the **ip local pool** command in global configuration mode. To delete address pools, use the **no** form of this command.

ip local pool *poolname first-address—last-address* [**mask** *mask*]

no ip local pool *poolname*

Syntax Description

first-address	Specifies the starting address in the range of IP addresses.
last-address	Specifies the final address in the range of IP addresses.
mask *mask*	(Optional) Specifies a subnet mask for the pool of addresses.
poolname	Specifies the name of the IP address pool.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You must supply the mask value when the IP addresses assigned to VPN clients belong to a non-standard network and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause some routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces. For example, if a printer, address 10.10.100.1/255.255.255.0 is available via interface 2, but the 10.10.10.0 network is available over the VPN tunnel and therefore interface 1, the VPN client would be confused as to where to route data destined for the printer. Both the 10.10.10.0 and 10.10.100.0 subnets fall under the 10.0.0.0 Class A network so the printer data may be sent over the VPN tunnel.

Examples

The following example configures an IP address pool named firstpool. The starting address is 10.20.30.40 and the ending address is 10.20.30.50. The network mask is 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

Related Commands

Command	Description
clear configure ip local pool	Removes all ip local pools.
show running-config ip local pool	Displays the ip pool configuration. To specify a specific IP address pool, include the name in the command.

ip-phone-bypass

To enable IP Phone Bypass, use the **ip-phone-bypass enable** command in group-policy configuration mode. To disable IP Phone Bypass, use the **ip-phone-bypass disable** command. To remove the IP phone Bypass attribute from the running configuration, use the **no** form of this command. This option allows inheritance of a value for IP Phone Bypass from another group policy.

IP Phone Bypass lets IP phones behind hardware clients connect without undergoing user authentication processes. If enabled, secure unit authentication remains in effect.

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

Syntax Description

disable	Disables IP Phone Bypass.
enable	Enables IP Phone Bypass.

Defaults

IP Phone Bypass is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You need to configure IP Phone Bypass only if you have enabled user authentication.

Examples

The following example shows how to enable IP Phone Bypass. for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-phone-bypass enable
```

Related Commands

Command	Description
user-authentication	Requires users behind a hardware client to identify themselves to the security appliance before connecting.

ips

The ASA 5500 series adaptive security appliance supports the AIP SSM, which runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

To assign traffic from the security appliance to the AIP SSM, use the **ips** command in class configuration mode. To remove this command, use the **no** form of this command.

ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**}

no ips {**inline** | **promiscuous**} {**fail-close** | **fail-open**}

Syntax Description

fail-close	Blocks traffic if the AIP SSM fails.
fail-open	Permits traffic if the AIP SSM fails.
inline	Directs packets to the AIP SSM; the packet might be dropped as a result of IPS operation.
promiscuous	Duplicates packets for the AIP SSM; the original packet cannot be dropped by the AIP SSM.

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**
Class configuration	•	•	—	—	•

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To configure the **ips** command, you must first configure the **class-map** command, **policy-map** command and the **class** command.

After you configure the security appliance to divert traffic to the AIP SSM, configure the AIP SSM inspection and protection policy, which determines how to inspect traffic and what to do when an intrusion is detected. You can either session to the AIP SSM from the security appliance (the **session** command) or you can connect directly to the AIP SSM using SSH or Telnet on its mangement interface. Alternatively, you can use ASDM. For more information about configuring the AIP SSM, see *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*.

Examples

The following example diverts all IP traffic to the AIP SSM in promiscous mode, and blocks all IP traffic should the AIP SSM card fail for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

Related Commands

Command	Description
class	Specifies a class map to use for traffic classification.
class-map	Identifies traffic for use in a policy map.
clear configure policy-map	Removes all **policy-map** configuration, except that if a policy map is in use in a **service-policy** command, that policy map is not removed.
policy-map	Configures a policy; that is, an association of a traffic class and one or more actions.
show running-config policy-map	Displays all current **policy-map** configurations.

ipsec-udp

To enable IPSec over UDP, use the **ipsec-udp enable** command in group-policy configuration mode. To disable IPSec over UDP, use the **ipsec-udp disable** command. To remove the IPSec over UDP attribute from the running configuration, use the **no** form of this command. This enables inheritance of a value for IPSec over UDP from another group policy.

IPSec over UDP, sometimes called IPSec through NAT, lets a Cisco VPN Client or hardware client connect via UDP to a security appliance that is running NAT.

ipsec-udp {enable | disable}

no ipsec-udp

Syntax Description

disable	Disables IPSec over UDP.
enable	Enables IPSec over UDP.

Defaults

IPSec over UDP is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

To use IPSec over UDP, you must also configure the **ipsec-udp-port** command.

The Cisco VPN Client must also be configured to use IPSec over UDP (it is configured to use it by default). The VPN 3002 requires no configuration to use IPSec over UDP.

IPSec over UDP is proprietary, it applies only to remote-access connections, and it requires mode configuration, means the security appliance exchanges configuration parameters with the client while negotiating SAs.

Using IPSec over UDP may slightly degrade system performance.

Examples

The following example shows how to set IPSec over UDP for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

Related Commands

Command	Description
ipsec-udp-port	Specifies the port on which the security appliance listens for UDP traffic.

ipsec-udp-port

To set a UDP port number for IPSec over UDP, use the **ipsec-udp-port** command in group-policy configuration mode. To disable the UDP port, use the **no** form of this command. This enables inheritance of a value for the IPSec over UDP port from another group policy.

In IPSec negotiations. the security appliance listens on the configured port and forwards UDP traffic for that port even if other filter rules drop UDP traffic.

ipsec-udp-port *port*

no ipsec-udp-port

Syntax Description

port	Identifies the UDP port number using an integer in the range 4001 through 49151.

Defaults

The default port is 10000.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

You can configure multiple group policies with this feature enabled, and each group policy can use a different port number.

Examples

The following example shows how to set an IPSec UDP port to port 4025 for the group policy named FirstGroup:

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

Related Commands

Command	Description
ipsec-udp	Lets a Cisco VPN Client or hardware client connect via UDP to a security appliance that is running NAT.

ip verify reverse-path

To enable Unicast RPF, use the **ip verify reverse-path** command in global configuration mode. To disable this feature, use the **no** form of this command. Unicast RPF guards against IP spoofing (a packet uses an incorrect source IP address to obscure its true source) by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

Syntax Description

interface_name	The interface on which you want to enable Unicast RPF.

Defaults

This feature is disabled by default.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Normally, the security appliance only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the security appliance to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the security appliance, the security appliance routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the security appliance can use the default route to satisfy the Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the security appliance uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, then the security appliance drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the security appliance drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.

- UDP and TCP have sessions, so the initial packet requires a reverse route lookup. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

Examples

The following example enables Unicast RPF on the outside interface:

```
hostname(config)# ip verify reverse-path interface outside
```

Related Commands

Command	Description
clear configure ip verify reverse-path	Clears the **ip verify reverse-path** configuration.
clear ip verify statistics	Clears the Unicast RPF statistics.
show ip verify statistics	Shows the Unicast RPF statistics.
show running-config ip verify reverse-path	Shows the **ip verify reverse-path** configuration.

ipv6 access-list

To configure an IPv6 access list, use the **ipv6 access-list** command in global configuration mode. To remove an ACE, use the **no** form of this command. Access lists define the traffic that the security appliance allows to pass through or blocks.

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} {*protocol* | **object-group** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} [*operator* {*port* [*port*] | **object-group** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [{*operator port* [*port*] | **object-group** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [**line** *line-num*] {**deny** | **permit**} **icmp6** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **object-group** *network_obj_grp_id*} {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **object-group** *network_obj_grp_id*} [*icmp_type* | **object-group** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

Syntax Description

any	An abbreviation for the IPv6 prefix ::/0, indicating any IPv6 address.
default	(Optional) Specifies that a syslog message 106100 is generated for the ACE.
deny	Denies access if the conditions are matched.
destination-ipv6-address	The IPv6 address of the host receiving the traffic.
destination-ipv6-prefix	The IPv6 network address where the traffic is destined.
disable	(Optional) Disables syslog messaging.
host	Indicates that the address refers to a specific host.
icmp6	Specifies that the access rule applies to ICMPv6 traffic passing through the security appliance.

icmp_type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect Omitting the *icmp_type* argument indicates all ICMP types.
icmp_type_obj_grp_id	(Optional) Specifies the object group ICMP type ID.
id	Name or number of an access list.
interval *secs*	(Optional) Specifies the time interval at which to generate an 106100 syslog message; valid values are from 1 to 600 seconds. The default interval is 300 seconds. This value is also used as the timeout value for deleting an inactive flow.
level	(Optional) Specifies the syslog level for message 106100; valid values are from 0 to 7. The default level is 6 (informational).
line *line-num*	(Optional) The line number where the access rule is being inserted into the list. If you do not specify a line number, the ACE is added to the end of the access list.
log	(Optional) Specifies the logging action for the ACE. If you do not specify the **log** keyword or you specify the **log default** keyword, then message 106023 is generated when a packet is denied by the ACE. If you sepcify the log keyword alone or with a level or interval, then message 106100 is generated when a packet is denied by the ACE. Packets that are denied by the implicit deny at the end of an access list are not logged. You must explicitly deny packets with an ACE to enable logging.
network_obj_grp_id	Existing network object group identification.
object-group	(Optional) Specifies an object group.

operator	(Optional) Specifies the operand to compare the source IP address to the destination IP address. The *operator* compares the source IP address or destination IP address ports. Possible operands include **lt** for less than, **gt** for greater than, **eq** for equal, **neq** for not equal, and **range** for an inclusive range. Use the **ipv6 access-list** command without an operator and port to indicate all ports by default.
permit	Permits access if the conditions are matched.
port	(Optional) Specifies the port that you permit or deny access. When entering the *port* argument, you can specify the port by either a number in the range of 0 to 65535 or a using literal name if the *protocol* is **tcp** or **udp**. Permitted TCP literal names are **aol, bgp**, **chargen**, **cifc**, **citrix-ica**, **cmd**, **ctiqbe**, **daytime**, **discard**, **domain**, **echo**, **exec**, **finger**, **ftp**, **ftp-data**, **gopher**, **h323**, **hostname**, **http**, **https**, **ident**, **irc**, **kerberos**, **klogin**, **kshell**, **ldap**, **ldaps**, **login**, **lotusnotes**, **lpd**, **netbios-ssn**, **nntp**, **pop2**, **pop3**, **pptp**, **rsh**, **rtsp**, **smtp**, **sqlnet**, **ssh**, **sunrpc, tacacs, talk, telnet, uucp, whois, and www**. Permitted UDP literal names are **biff**, **bootpc**, **bootps**, **cifs**, **discard**, **dnsix**, **domain**, **echo**, **http**, **isakmp**, **kerberos**, **mobile-ip**, **nameserver**, **netbios-dgm**, **netbios-ns**, **ntp**, **pcanywhere-status**, **pim-auto-rp**, **radius**, **radius-acct**, **rip**, **secureid-udp**, **snmp**, **snmptrap**, **sunrpc**, **syslog**, **tacacs**, **talk**, **tftp**, **time**, **who**, **www**, and **xdmcp**.
prefix-length	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).
protocol	Name or number of an IP protocol; valid values are **icmp**, **ip**, **tcp**, or **udp**, or an integer in the range 1 to 254 representing an IP protocol number.
protocol_obj_grp_id	Existing protocol object group identification.
service_obj_grp_id	(Optional) Specifies the object group.
source-ipv6-address	The IPv6 address of the host sending the traffic.
source-ipv6-prefix	The IPv6 network address of the where the network traffic originated.

Defaults

When the **log** keyword is specified, the default level for syslog message 106100 is 6 (informational).

The default logging interval is 300 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command allows you to specify if an IPv6 address is permitted or denied access to a port or protocol. Each command is called an ACE. One or more ACEs with the same access list name are referred to as an access list. Apply an access list to an interface using the **access-group** command.

The security appliance denies all packets from an outside interface to an inside interface unless you specifically permit access using an access list. All packets are allowed by default from an inside interface to an outside interface unless you specifically deny access.

The **ipv6 access-list** command is similar to the **access-list** command, except that it is IPv6-specific. For additional information about access lists, refer to the **access-list extended** command.

The **ipv6 access-list icmp** command is used to filter ICMPv6 messages that pass through the security appliance.To configure the ICMPv6 traffic that is allowed to originate and terminate at a specific interface, use the **ipv6 icmp** command.

Refer to the **object-group** command for information on how to configure object groups.

Examples

The following example will allow any host using TCP to access the 3001:1::203:A0FF:FED6:162D server:

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host 3001:1::203:A0FF:FED6:162D
```

The following example uses **eq** and a port to deny access to just FTP:

```
hostname(config)# ipv6 access-list acl_out deny tcp any host 3001:1::203:A0FF:FED6:162D eq
ftp
hostname(config)# access-group acl_out in interface inside
```

The following example uses **lt** to permit access to all ports less than port 2025, which permits access to the well-known ports (1 to 1024):

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host 3001:1::203:A0FF:FED6:162D
lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

Related Commands

Command	Description
access-group	Assigns an access list to an interface.
ipv6 icmp	Configures access rules for ICMP messages that terminate at an interface of the security appliance.
object-group	Creates an object group (addresses, ICMP types, and services).

ipv6 address

To enable IPv6 and configure the IPv6 addresses on an interface, use the **ipv6 address** command in interface configuration mode. To remove the IPv6 addresses, use the **no** form of this command.

ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

no ipv6 address {**autoconfig** | *ipv6-prefix*/*prefix-length* [**eui-64**] | *ipv6-address* **link-local**}

Syntax Description

autoconfig	Enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface.
eui-64	(Optional) Specifies an interface ID in the low order 64 bits of the IPv6 address.
ipv6-address	The IPv6 link-local address assigned to the interface.
ipv6-prefix	The IPv6 network address assigned to the interface.
link-local	Specifies that the address is a link-local address.
prefix-length	Indicates how many of the high-order, contiguous bits of the address comprise the IPv6 prefix (the network portion of the IPv6 address).

Defaults

IPv6 is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Configuring an IPv6 address on an interface enables IPv6 on that interface; you do not need to use the **ipv6 enable** command after specifying an IPv6 address.

The **ipv6 address autoconfig** command is used to enable automatic configuration of IPv6 addresses on an interface using stateless autoconfiguration. The addresses are configured based on the prefixes received in Router Advertisement messages. If a link-local address has not been configured, then one is automatically generated for this interface. An error message is displayed if another host is using the link-local address.

The **ipv6 address eui-64** command is used to configure an IPv6 address for an interface. If the optional **eui-64** is specified, the EUI-64 interface ID will be used in the low order 64 bits of the address. If the value specified for the *prefix-length* argument is greater than 64 bits, the prefix bits have precedence over the interface ID. An error message will be displayed if another host is using the specified address.

The Modified EUI-64 format interface ID is derived from the 48-bit link-layer (MAC) address by inserting the hex number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure the chosen address is from a unique Ethernet MAC address, the next-to-lowest order bit in the high-order byte is inverted (universal/local bit) to indicate the uniqueness of the 48-bit address. For example, an interface with a MAC address of 00E0.B601.3B7A would have a 64 bit interface ID of 02E0:B6FF:FE01:3B7A.

The **ipv6 address link-local** command is used to configure an IPv6 link-local address for an interface. The *ipv6-address* specified with this command overrides the link-local address that is automatically generated for the interface. The link-local address is composed of the link-local prefix FE80::/64 and the interface ID in Modified EUI-64 format. An interface with a MAC address of 00E0.B601.3B7A would have a link-local address of FE80::2E0:B6FF:FE01:3B7A. An error message will be displayed if another host is using the specified address.

Examples

The following example assigns 3FFE:C00:0:1::576/64 as the global address for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

The following example assigns an IPv6 address automatically for the selected interface:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

The following example assigns IPv6 address 3FFE:C00:0:1::/64 to the selected interface and specifies an EUI-64 interface ID in the low order 64 bits of the address:

```
hostname(config)# interface gigabitethernet 0/2
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

The following example assigns FE80::260:3EFF:FE11:6670 as the link-level address for the selected interface:

```
hostname(config)# interface gigabitethernet 0/3
hostname(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

Related Commands

Command	Description
debug ipv6 interface	Displays debug information for IPv6 interfaces.
show ipv6 interface	Displays the status of interfaces configured for IPv6.

ipv6 enable

To enable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **ipv6 enable** command in interface configuration mode. To disable IPv6 processing on an interface that has not been configured with an explicit IPv6 address, use the **no** form of this command.

ipv6 enable

no ipv6 enable

Syntax Description

This command has no arguments or keywords.

Defaults

IPv6 is disabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 enable** command automatically configures an IPv6 link-local unicast address on the interface while also enabling the interface for IPv6 processing.

The **no ipv6 enable** command does not disable IPv6 processing on an interface that is configured with an explicit IPv6 address.

Examples

The following example enables IPv6 processing on the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address for an interface and enables IPv6 processing on the interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 icmp

To configure ICMP access rules for an interface, use the **ipv6 icmp** command in global configuration mode. To remove an ICMP access rule, use the **no** form of this command.

ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {**permit** | **deny**} {*ipv6-prefix*/*prefix-length* | **any** | **host** *ipv6-address*} [*icmp-type*] *if-name*

Syntax Description

any	Keyword specifying any IPv6 address. An abbreviation for the IPv6 prefix ::/0.
deny	Prevents the specified ICMP traffic on the selected interface.
host	Indicates that the address refers to a specific host.
icmp-type	Specifies the ICMP message type being filtered by the access rule. The value can be a valid ICMP type number (from 0 to 255) or one of the following ICMP type literals: • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	The name of the interface, as designated by the **nameif** command, the access rule applies to.
ipv6-address	The IPv6 address of the host sending ICMPv6 messages to the interface.
ipv6-prefix	The IPv6 network that is sending ICMPv6 messages to the interface.
permit	Allows the specified ICMP traffic on the selected interface.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Defaults

If no ICMP access rules are defined, all ICMP traffic is permitted.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

ICMP in IPv6 functions the same as ICMP in IPv4. ICMPv6 generates error messages, such as ICMP destination unreachable messages and informational messages like ICMP echo request and reply messages. Additionally, ICMP packets in IPv6 are used in the IPv6 neighbor discovery process and path MTU discovery.

If there are no ICMP rules defined for an interface, all IPv6 ICMP traffic is permitted.

If there are ICMP rules defined for an interface, then the rules are processed in order on a first-match basis followed by an implicit deny all rule. For example, if the first matched rule is a permit rule, the ICMP packet is processed. If the first matched rule is a deny rule, or if the ICMP packet did not match any rule on that interface, then the security appliance discards the ICMP packet and generates a syslog message.

For this reason, the order that you enter the ICMP rules is important. If you enter a rule denying all ICMP traffic from a specific network, and then follow it with a rule permitting ICMP traffic from a particular host on that network, the host rule will never be processed. The ICMP traffic is blocked by the network rule. However, if you enter the host rule first, followed by the network rule, the host ICMP traffic will be allowed, while all other ICMP traffic from that network is blocked.

The **ipv6 icmp** command configures access rules for ICMP traffic that terminates at the security appliance interfaces. To configure access rules for pass-through ICMP traffic, refer to the **ipv6 access-list** command.

Examples

The following example denies all ping requests and permits all Packet Too Big messages (to support Path MTU Discovery) at the outside interface:

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

The following example permits host 2000:0:0:4::2 or hosts on prefix 2001::/64 to ping the outside interface:

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

Related Commands

Command	Description
ipv6 access-list	Configures access lists.

ipv6 nd dad attempts

To configure the number of consecutive neighbor solicitation messages that are sent on an interface during duplicate address detection, use the **ipv6 nd dad attempts** command in interface configuration mode. To return to the default number of duplicate address detection messages sent, use the **no** form of this command.

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

Syntax Description

value	A number from 0 to 600. Entering 0 disables duplicate address detection on the specified interface. Entering 1 configures a single transmission without follow-up transmissions. The default value is 1 message.

Defaults

The default number of attempts is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Duplicate address detection verifies the uniqueness of new unicast IPv6 addresses before the addresses are assigned to interfaces (the new addresses remain in a tentative state while duplicate address detection is performed). Duplicate address detection uses neighbor solicitation messages to verify the uniqueness of unicast IPv6 addresses. The frequency at which the neighbor solicitation messages are sent is configured using the **ipv6 nd ns-interval** command.

Duplicate address detection is suspended on interfaces that are administratively down. While an interface is administratively down, the unicast IPv6 addresses assigned to the interface are set to a pending state.

Duplicate address detection is automatically restarted on an interface when the interface returns to being administratively up. An interface returning to administratively up restarts duplicate address detection for all of the unicast IPv6 addresses on the interface.

Note While duplicate address detection is performed on the link-local address of an interface, the state for the other IPv6 addresses is still set to tentative. When duplicate address detection is completed on the link-local address, duplicate address detection is performed on the remaining IPv6 addresses.

When duplicate address detection identifies a duplicate address, the state of the address is set to DUPLICATE and the address is not used. If the duplicate address is the link-local address of the interface, the processing of IPv6 packets is disabled on the interface and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

If the duplicate address is a global address of the interface, the address is not used and an error message similar to the following is issued:

```
%PIX-4-DUPLICATE: Duplicate address 3000::4 on outside
```

All configuration commands associated with the duplicate address remain as configured while the state of the address is set to DUPLICATE.

If the link-local address for an interface changes, duplicate address detection is performed on the new link-local address and all of the other IPv6 address associated with the interface are regenerated (duplicate address detection is performed only on the new link-local address).

Examples

The following example configures 5 consecutive neighbor solicitation messages to be sent when duplicate address detection is being performed on the tentative unicast IPv6 address of the interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

The following example disables duplicate address detection on the selected interface:

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

Related Commands

Command	Description
ipv6 nd ns-interval	Configures the interval between IPv6 neighbor solicitation transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ns-interval

To configure the interval between IPv6 neighbor solicitation retransmissions on an interface, use the **ipv6 nd ns-interval** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

Syntax Description

value	The interval between IPv6 neighbor solicitation transmissions, in milliseconds. Valid values range from 1000 to 3600000 milliseconds. The default value is 1000 milliseconds.

Defaults

1000 milliseconds between neighbor solicitation transmissions.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This value will be included in all IPv6 router advertisements sent out this interface.

Examples

The following example configures an IPv6 neighbor solicitation transmission interval of 9000 milliseconds for Gigabitethernet 0/0:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd prefix

To configure which IPv6 prefixes are included in IPv6 router advertisements, use the **ipv6 nd prefix** command in interface configuration mode. To remove the prefixes, use the **no** form of this command.

ipv6 nd prefix *ipv6-prefix*/*prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

no ipv6 nd prefix *ipv6-prefix*/*prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

Syntax Description

at *valid-date preferred-date*	The date and time at which the lifetime and preference expire. The prefix is valid until this specified date and time are reached. Dates are expressed in the form *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire*.
default	Default values are used.
infinite	(Optional) The valid lifetime does not expire.
ipv6-prefix	The IPv6 network number to include in router advertisements. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
no-advertise	(Optional) Indicates to hosts on the local link that the specified prefix is not to be used for IPv6 autoconfiguration.
no-autoconfig	(Optional) Indicates to hosts on the local link that the specified prefix cannot be used for IPv6 autoconfiguration.
off-link	(Optional) Indicates that the specified prefix is not used for on-link determination.
preferred-lifetime	The amount of time (in seconds) that the specified IPv6 prefix is advertised as being preferred. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with infinite. The default is 604800 (7 days).
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.
valid-lifetime	The amount of time that the specified IPv6 prefix is advertised as being valid. Valid values range from 0 to 4294967295 seconds. The maximum value represents infinity, which can also be specified with **infinite**. The default is 2592000 (30 days).

Defaults

All prefixes configured on interfaces that originate IPv6 router advertisements are advertised with a valid lifetime of 2592000 seconds (30 days) and a preferred lifetime of 604800 seconds (7 days), and with both the “onlink” and “autoconfig” flags set.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

This command allows control over the individual parameters per prefix, including whether or not the prefix should be advertised.

By default, prefixes configured as addresses on an interface using the **ipv6 address** command are advertised in router advertisements. If you configure prefixes for advertisement using the **ipv6 nd prefix** command, then only these prefixes are advertised.

The **default** keyword can be used to set default parameters for all prefixes.

A date can be set to specify the expiration of a prefix. The valid and preferred lifetimes are counted down in real time. When the expiration date is reached, the prefix will no longer be advertised.

When onlink is "on" (by default), the specified prefix is assigned to the link. Nodes sending traffic to such addresses that contain the specified prefix consider the destination to be locally reachable on the link.

When autoconfig is "on" (by default), it indicates to hosts on the local link that the specified prefix can be used for IPv6 autoconfiguration.

Examples

The following example includes the IPv6 prefix 2001:200::/35, with a valid lifetime of 1000 seconds and a preferred lifetime of 900 seconds, in router advertisements sent out on the specified interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address and enables IPv6 processing on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-interval

To configure the interval between IPv6 router advertisement transmissions on an interface, use the **ipv6 nd ra-interval** command in interface configuration mode. To restore the default interval, use the **no** form of this command.

ipv6 nd ra-interval [**msec**] *value*

no ipv6 nd ra-interval [[**msec**] *value*]

Syntax Description

msec	(Optional) indicates that the value provided is in milliseconds. If this keyword is not present, the value provided is seconds.
value	The interval between IPv6 router advertisement transmissions. Valid values range from 3 to 1800 seconds, or from 500 to 1800000 milliseconds if the **msec** keyword is provided. The default is 200 seconds.

Defaults

200 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The interval between transmissions should be less than or equal to the IPv6 router advertisement lifetime if the security appliance is configured as a default router by using the **ipv6 nd ra-lifetime** command. To prevent synchronization with other IPv6 nodes, randomly adjust the actual value used to within 20 percent of the specified value.

Examples

The following example configures an IPv6 router advertisement interval of 201 seconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-interval 201
```

Related Commands

Command	Description
ipv6 nd ra-lifetime	Configures the lifetime of an IPv6 router advertisement.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd ra-lifetime

To configure the "router lifetime" value in IPv6 router advertisements on an interface, use the **ipv6 nd ra-lifetime** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

Syntax Description

seconds	The validity of the security appliance as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the security appliance should not be considered a default router on the selected interface.

Defaults

1800 seconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The "router lifetime" value is included in all IPv6 router advertisements sent out the interface. The value indicates the usefulness of the security appliance as a default router on this interface.

Setting the value to a non-zero value to indicates that the security appliance should be considered a default router on this interface. The no-zero value for the "router lifetime" value should not be less than the router advertisement interval.

Setting the value to 0 indicates that the security appliance should not be considered a default router on this interface.

Examples

The following example configures an IPv6 router advertisement lifetime of 1801 seconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

Related Commands

Command	Description
ipv6 nd ra-interval	Configures the interval between IPv6 router advertisement transmissions on an interface.
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd reachable-time

To configure the amount of time that a remote IPv6 node is considered reachable after a reachability confirmation event has occurred, use the **ipv6 nd reachable-time** command in interface configuration mode. To restore the default time, use the **no** form of this command.

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

Syntax Description

value	The amount of time, in milliseconds, that a remote IPv6 node is considered reachable. Valid values range from 0 to 3600000 milliseconds. The default is 0.

Defaults

0 milliseconds.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The configured time enables detecting unavailable neighbors. Shorter configured times enable detecting unavailable neighbors more quickly; however, shorter times consume more IPv6 network bandwidth and processing resources in all IPv6 network devices. Very short configured times are not recommended in normal IPv6 operation.

Examples

The following example configures an IPv6 reachable time of 1700000 milliseconds for the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 nd suppress-ra

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra** command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Defaults

Router advertisements are automatically sent on LAN interfaces if IPv6 unicast routing is enabled.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **no ipv6 nd suppress-ra** command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on the selected interface:

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor

To configure a static entry in the IPv6 neighbor discovery cache, use the **ipv6 neighbor** command in global configuration mode. To remove a static entry from the neighbor discovery cache, use the **no** form of this command.

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

Syntax Description

if_name	The internal or external interface name designated by the **nameif** command.
ipv6_address	The IPv6 address that corresponds to the local data-link address.
mac_address	The local data-line (hardware MAC) address.

Defaults

Static entries are not configured in the IPv6 neighbor discovery cache.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 neighbor** command is similar to the **arp** command. If an entry for the specified IPv6 address already exists in the neighbor discovery cache—learned through the IPv6 neighbor discovery process—the entry is automatically converted to a static entry. These entries are stored in the configuration when the **copy** command is used to store the configuration.

Use the **show ipv6 neighbor** command to view static entries in the IPv6 neighbor discovery cache.

The **clear ipv6 neighbors** command deletes all entries in the IPv6 neighbor discovery cache except static entries. The **no ipv6 neighbor** command deletes a specified static entry from the neighbor discovery cache; the command does not remove dynamic entries—entries learned from the IPv6 neighbor discovery process—from the cache. Disabling IPv6 on an interface by using the **no ipv6 enable** command deletes all IPv6 neighbor discovery cache entries configured for that interface except static entries (the state of the entry changes to INCMP [Incomplete]).

Static entries in the IPv6 neighbor discovery cache are not modified by the neighbor discovery process.

Examples

The following example adds a static entry for the an inside host with an IPv6 address of 3001:1::45A and a MAC address of 0002.7D1A.9472 to the neighbor discovery cache:

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

Related Commands

Command	Description
clear ipv6 neighbors	Deletes all entries in the IPv6 neighbor discovery cache, except static entries.
show ipv6 neighbor	Displays IPv6 neighbor cache information.

ipv6 route

To add an IPv6 route to the IPv6 routing table, use the **ipv6 route** command in global configuration mode. To remove an IPv6 default route, use the **no** form of this command.

ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance*]

no ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance*]

Syntax Description

administrative-distance	(Optional) The administrative distance of the route. The default value is 1, which gives static routes precedence over any other type of routes except connected routes.
if_name	The name of the interface the route is being configured for.
ipv6-address	The IPv6 address of the next hop that can be used to reach the specified network.
ipv6-prefix	The IPv6 network that is the destination of the static route. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
prefix-length	The length of the IPv6 prefix. This value indicates how many of the high-order, contiguous bits of the address comprise the network portion of the prefix. The slash (/) must precede the prefix length.

Defaults

By default, the *administrative-distance* is 1.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

Use the **show ipv6 route** command to view the contents of the IPv6 routing table.

Examples

The following example routes packets for network 7fff::0/32 to a networking device on the inside interface at 3FFE:1100:0:CC00::1 with an administrative distance of 110:

```
hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

Related Commands

Command	Description
debug ipv6 route	Displays debug messages for IPv6 routing table updates and route cache updates.
show ipv6 route	Displays the current contents of the IPv6 routing table.

isakmp am-disable

To disable inbound aggressive mode connections, use the **isakmp am-disable** command in global configuration mode. To enable inbound aggressive mode connections, use the **no** form of this command.

isakmp am-disable

no isakmp am-disable

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is enabled.

Command Modes

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

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

Command History

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

Examples

The following example, entered in global configuration mode, disables inbound aggressive mode connections:

```
hostname(config)# isakmp am-disable
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp disconnect-notify

To enable disconnect notification to peers, use the **isakmp disconnect-notify** command in global configuration mode. To disable disconnect notification, use the **no** form of this command.

isakmp disconnect-notify

no isakmp disconnect-notify

Syntax Description

This command has no arguments or keywords.

Defaults

The default value is disabled.

Command Modes

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

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

Command History

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

Examples

The following example, entered in global configuration mode, enables disconnect notification to peers:

```
hostname(config)# isakmp disconnect-notify
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp enable

To enable ISAKMP negotiation on the interface on which the IPSec peer communicates with the security appliance, use the **isakmp enable** command in global configuration mode. To disable ISAKMP on the interface, use the **no** form of this command.

isakmp enable *interface-name*

no isakmp enable *interface-name*

Syntax Description

interface-name	Specifies the name of the interface on which to enable or disable ISAKMP negotiation.

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.

Examples

The following example, entered in global configuration mode, shows how to disable ISAKMP on the inside interface:

```
hostname(config)# no isakmp enable inside
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp identity

To set the Phase 2 ID to be sent to the peer, use the **isakmp identity** command in global configuration mode. To return to the default setting, use the **no** form of this command.

isakmp identity {address | hostname | key-id *key-id-string* **| auto}**

no isakmp identity {address | hostname | key-id *key-id-string* **| auto}**

Syntax Description

address	Uses the IP address of the host exchanging ISAKMP identity information.
auto	Determines ISKMP negotiation by connection type; IP address for preshared key or cert DN for certificate authentication.
hostname	Uses the fully-qualified domain name of the host exchanging ISAKMP identity information (default). This name comprises the hostname and the domain name.
key-id *key_id_string*	Specifies the string used by the remote peer to look up the preshared key.

Defaults

The default ISAKMP identity is **isakmp identity hostname**.

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.

Examples

The following example, entered in global configuration mode, enables ISAKMP negotiation on the interface for communicating with the IPSec peer, depending on connection type:

```
hostname(config)# isakmp identity auto
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.

Command	Description
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp ipsec-over-tcp

To enable IPSec over TCP, use the **isakmp ipsec-over-tcp** command in global configuration mode. To disable IPSec over TCP, use the **no** form of this command.

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

Syntax Description

port *port1...port10*	(Optional) Specifies the ports on which the device accepts IPSec over TCP connections. You can list up to 10 ports. Port numbers can be in the range 1-65535. The default port number is 10000.

Defaults

The default value is disabled.

Command Modes

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

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

Command History

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

Examples

This example, entered in global configuration mode, enables IPSec over TCP on port 45:

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp keepalive

To configure IKE DPD, use the **isakmp keepalive** command in tunnel-group ipsec-attributes configuration mode. In every tunnel group, IKE keepalives are enabled by default with default threshold and retry values. To return the keepalive parameters to enabled with default threshold and retry values, use the **no** form of this command.

isakmp keepalive [**threshold** *seconds*] [**retry** *seconds*] [**disable**]

no isakmp keepalive disable

Syntax Description

disable	Disables IKE keepalive processing, which is enabled by default.
retry *seconds*	Specifies the interval in seconds between retries after a keepalive response has not been received. The range is 2-10 seconds. The default is 2 seconds.
threshold *seconds*	Specifies the number of seconds the peer can idle before beginning keepalive monitoring. The range is 10-3600 seconds. The default is 10 seconds for a LAN-to-LAN group, and 300 second for a remote access group.

Defaults

The default for a remote access group is a threshold of 300 seconds and a retry of 2 seconds.

For a LAN-to-LAN group, the default is a threshold of 10 seconds and a retry of 2 seconds.

Command Modes

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

	Firewall Mode		Security Context		
				Multiple	
Command Mode	**Routed**	**Transparent**	**Single**	**Context**	**System**
Tunnel-group ipsec attributes configuration	•	—	•	—	—

Command History

Release	Modification
7.0(1)	This command was introduced.

Usage Guidelines

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

Examples

The following example entered in config-ipsec configuration mode, configures IKE DPD, establishes a threshold of 15, and specifies a retry interval of 10 for the IPSec LAN-to-LAN tunnel group with the IP address 209.165.200.225:

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

Related Commands

Command	Description
clear-configure tunnel-group	Clears all configured tunnel groups.
show running-config tunnel-group	Shows the tunnel group configuration for all tunnel groups or for a particular tunnel group.
tunnel-group ipsec-attributes	Configures the tunnel-group ipsec-attributes for this group.

isakmp nat-traversal

To enable NAT traversal globally, check that ISAKMP is enabled (you can enable it with the **isakmp enable** command) in global configuration mode and then use the **isakmp nat-traversal** command. If you have enabled NAT traversal, you can disable it with the **no** form of this command.

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

Syntax Description

natkeepalive	Sets the NAT keep alive interval, from 10 to 3600 seconds. The default is 20 seconds.

Defaults

By default, NAT traversal (**isakmp nat-traversal**) is disabled.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting.

Usage Guidelines

Network Address Translation (NAT), including Port Address Translation (PAT), is used in many networks where IPSec is also used, but there are a number of incompatibilities that prevent IPSec packets from successfully traversing NAT devices. NAT traversal enables ESP packets to pass through one or more NAT devices.

The security appliance supports NAT traversal as described by Version 2 and Version 3 of the IETF "UDP Encapsulation of IPsec Packets" draft, available at http://www.ietf.org/html.charters/ipsec-charter.html, and NAT traversal is supported for both dynamic and static crypto maps.

This command enables NAT-T globally on the security appliance. To disable in a crypto-map entry, use the **crypto map set nat-t-disable** command.

Examples

The following example, entered in global configuration mode, enables ISAKMP and then enables NAT traversal with an interval of 30 seconds:

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy authentication

To specify an authentication method within an IKE policy, use the **isakmp policy authentication** command in global configuration mode. IKE policies define a set of parameters for IKE negotiation. To reset the authentication method to the default value, use the **no** form of this command.

isakmp policy *priority* **authentication** {**pre-share | dsa-sig | rsa-sig**}

no isakmp policy *priority* **authentication**

Syntax Description

dsa-sig	Specifies DSA signatures as the authentication method.
pre-share	Specifies preshared keys as the authentication method.
priority	Uniquely identifies the IKE policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
rsa-sig	Specifies RSA signatures as the authentication method. RSA signatures provide non-repudiation for the IKE negotiation. This basically means you can prove to a third party whether you had an IKE negotiation with the peer.

Defaults

The default ISAKMP policy authentication is **pre-share**.

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. DSA-Sig was added in 7.0.

Usage Guidelines

If you specify RSA signatures, you must configure the security appliance and its peer to obtain certificates from a certification authority (CA). If you specify preshared keys, you must separately configure these preshared keys within the security appliance and its peer.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy authentication** command. This example sets the authentication method of RSA Signatures to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 authentication rsa-sig
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy encryption

To specify the encryption algorithm to use within an IKE policy, use the **isakmp policy encryption** command in global configuration mode. To reset the encryption algorithm to the default value, which is **des,** use the **no** form of this command.

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

Syntax Description

3des	Specifies that the Triple DES encryption algorithm be used in the IKE policy.
aes	Specifies that the encryption algorithm to use in the IKE policy is AES with a 128-bit key.
aes-192	Specifies that the encryption algorithm to use in the IKE policy is AES with a 192-bit key.
aes-256	Specifies that the encryption algorithm to use in the IKE policy is AES with a 256-bit key.
des	Specifies that the encryption algorithm to use in the IKE policy is 56-bit DES-CBC.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default ISAKMP policy encryption is **3des**.

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.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy encryption** command; it sets 128-bit key AES encryption as the algorithm to be used within the IKE policy with the priority number of 25.

```
hostname(config)# isakmp policy 25 encryption aes
```

The following example, entered in global configuration mode, sets the 3DES algorithm to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 encryption 3des
```

```
hostname(config)#
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy group

To specify the Diffie-Hellman group for an IKE policy, use the **isakmp policy group** command in global configuration mode. IKE policies define a set of parameters to use during IKE negotiation. To reset the Diffie-Hellman group identifier to the default value, use the **no** form of this command.

isakmp policy *priority* **group** {**1** | **2** | **5** | **7**}

no isakmp policy *priority* **group**

Syntax Description

group 1	Specifies that the 768-bit Diffie-Hellman group be used in the IKE policy. This is the default value.
group 2	Specifies that the 1024-bit Diffie-Hellman group 2 be used in the IKE policy.
group 5	Specifies that the 1536-bit Diffie-Hellman group 5 be used in the IKE policy.
group 7	Specifies that Diffie-Hellman Group 7 be used in the IKE policy. Group 7 generates IPSec SA keys, where the elliptical curve field size is 163 bits.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.

Defaults

The default group policy is group 2.

Command Modes

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

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

Command History

Release	Modification
Preexisting	This command was preexisting. Group 7 was added.

Usage Guidelines

There are four group options: 768-bit (DH Group 1), 1024-bit (DH Group 2), 1536-bit (DH Group 5), and DH Group 7. The 1024-bit and 1536-bit Diffie-Hellman Groups provide stronger security, but require more CPU time to execute.

Note The Cisco VPN Client Version 3.x or higher requires **isakmp policy** to have DH **group 2** configured. (If you have DH **group 1** configured, the Cisco VPN Client cannot connect.)

AES support is available on security appliances licensed for VPN-3DES only. Due to the large key sizes provided by AES, ISAKMP negotiation should use Diffie-Hellman (DH) **group 5** instead of **group 1** or **group 2**. This is done with the **isakmp policy priority group 5** command.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy group** command. This example sets group 2, the 1024-bit Diffie Hellman, to be used within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 group 2
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy hash

To specify the hash algorithm for an IKE policy, use the **isakmp policy hash** command in global configuration mode. IKE policies define a set of parameters to be used during IKE negotiation.

To reset the hash algorithm to the default value of SHA-1, use the **no** form of this command.

isakmp policy *priority* **hash** {**md5** | **sha**}

no isakmp policy *priority* **hash**

Syntax Description

md5	Specifies that MD5 (HMAC variant) as the hash algorithm be used in the IKE policy.
priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
sha	Specifies that SHA-1 (HMAC variant) as the hash algorithm be used in the IKE policy.

Defaults

The default hash algorithm is SHA-1 (HMAC variant).

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

There are two hash algorithm options: SHA-1 and MD5. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.

Examples

The following example, entered in global configuration mode, shows use of the **isakmp policy hash** command. This example specifies that the MD5 hash algorithm be used within the IKE policy, with the priority number of 40.

```
hostname(config)# isakmp policy 40 hash md5
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp policy lifetime

To specify the lifetime of an IKE security association before it expires, use the **isakmp policy lifetime** command in global configuration mode. You can specify an infinite lifetime if the peer does not propose a lifetime. Use the **no** form of this command to reset the security association lifetime to the default value of 86,400 seconds (one day).

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

Syntax Description

priority	Uniquely identifies the Internet Key Exchange (IKE) policy and assigns a priority to the policy. Use an integer from 1 to 65,534, with 1 being the highest priority and 65,534 the lowest.
seconds	Specifies how many seconds each security association should exist before expiring. To propose a finite lifetime, use an integer from 120 to 2147483647 seconds. Use 0 seconds for infinite lifetime.

Defaults

The default value is 86,400 seconds (one day).

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 IKE begins negotiations, it seeks to agree upon the security parameters for its own session. Then the security association at each peer refers to the agreed-upon parameters. The peers retain the security association until the lifetime expires. Before a security association expires, subsequent IKE negotiations can use it, which can save time when setting up new IPSec security associations. The peers negotiate new security associations before current security associations expire.

With longer lifetimes, the security appliance sets up future IPSec security associations more quickly. Encryption strength is great enough to ensure security without using very fast rekey times, on the order of every few minutes. We recommend that you accept the default.

Note If the IKE security association is set to an infinite lifetime, but the peer proposes a finite lifetime, then the negotiated finite lifetime from the peer is used.
The following example, entered in global configuration mode, shows use of the **isakmp policy lifetime** command. This example sets the lifetime of the IKE security association to 50,400 seconds (14 hours) within the IKE policy with the priority number of 40.

Examples

The following example, entered in global configuration mode, sets the lifetime of the IKE security association to 50,4000 seconds (14 hours) within the IKE policy with the priority number of 40.

```
hostname(config)# isakmp policy 40 lifetime 50400
```

The following example, entered in global configuration mode, sets the IKE security association to an infinite lifetime.

```
hostname(config)# isakmp policy 40 lifetime 0
```

Related Commands

clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

isakmp reload-wait

To enable waiting for all active sessions to voluntarily terminate before rebooting the security appliance, use the **isakmp reload-wait** command in global configuration mode. To disable waiting for active sessions to terminate and to proceed with a reboot of the security appliance, use the **no** form of this command.

isakmp reload-wait

no isakmp reload-wait

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
7.0(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, tells the security appliance to wait until all active sessions have terminated before rebooting.

```
hostname(config)# isakmp reload-wait
```

Related Commands

Command	Description
clear configure isakmp	Clears all the ISAKMP configuration.
clear configure isakmp policy	Clears all ISAKMP policy configuration.
clear isakmp sa	Clears the IKE runtime SA database.
show running-config isakmp	Displays all the active configuration.

issuer-name

To identify the DN from the CA certificate to be compared to the rule entry string, use the **issuer-name** command in CA certificate map configuration mode. To remove an issuer-name, use the **no** form of the command.

issuer-name [**attr** *tag*] {**eq | ne | co | nc**} *string*

no issuer-name [**attr** *tag*] {**eq | ne | co | nc**} *string*

Syntax Description

attr *tag*	Indicates that only the specified attribute value form the certificate DN string will be compared to the rule entry string. The tag values are as follows: DNQ = DN qualifier GENQ = Generational qualifier I = Initials GN = Given name N = Name SN = Surname IP = IP address SER = Serial number UNAME = Unstructured name EA = Email address T = Title O = Organization Name L = Locality SP = State/Province C = Country OU = Organizational unit CN = Common name
co	Specifies that the DN string or indicated attribute must be a substring in the rule entry string.
eq	Specifies that the DN string or indicated attribute must match the entire rule string.
nc	Specifies that the DN string or indicated attribute must not be a substring in the rule entry string.
ne	Specifies that the DN string or indicated attribute must not match the entire rule string.
string	Specifies the rule entry information.

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.

Examples

The following example enters the CA certificate map mode for certificate map 4 and configures the issuer name as O = central:

```
hostname(config)# crypto ca certificate map 4
hostname(ca-certificate-map)# issuer-name attr o eq central
hostname(ca-certificate-map)# exit
```

Related Commands

Command	Description
crypto ca certificate map	Enters CA certificate map mode.
subject-name (crypto ca certificate map)	Identifies the DN from the CA certificate that is to be compared to the rule entry string.