CHAPTER 16

interface through issuer-name Commands

interface

To add an interface to the configuration and enter interface configuration mode, use the **interface** command in global configuration mode.

interface {*vlan <n>* | *mapped_name*}

Syntax Description

mapped_name	(Optional) In multiple context mode, identifies the mapped name if it was assigned using the **allocate-interface** command.
vlan <n>	In multiple context mode, lets you configure the name, sec level, IP address of the VLAN.

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
1.1(1)	This command was introduced.
2.2(1)	This command was changed.
3.1(1)	This command was modified to change arguments to be separate commands under interface configuration mode.

Usage Guidelines

In multimode in the system, you can allocate interfaces to context which allows the FWSM to add them; you do not need to manually add interfaces. Similarly, if you assign a VLAN to the failover or state link, the **interface** command is added automatically.

In single mode, you need to enter the interface command for a given VLAN, to set parameters for it.

In interface configuration mode, you can assign a name, assign a VLAN, assign an IP address, and configure many other settings. If you add an interface for a VLAN that is not yet assigned to the FWSM by the switch, the interface will be in the down state. When you assign the VLAN to the FWSM, the interface changes to an up state. See the show interface command for more information about interface states.

When you assign a VLAN to a context using the **allocate-interface** command, the FWSM automatically adds the interface to the system configuration, if it is not already present. For example, when you allocate 'VLAN 100' to a context, the **interface vlan 100** command is added to the system configuration.

The **failover lan interface** *interface_name* **vlan** *vlan* command specifies the interface name and the VLAN used for communication between the active and the standby modules to determine the operating status of each module.

The **failover link** *interface_name* [**vlan** *vlan*] command specifies the interface name and VLAN for the stateful failover interface. The link passes all protocol state information between the active and the standby for stateful failover.

Examples

The following example shows how to enter the interface configuration mode:

```
fwsm(config)# interface vlan22
fwsm(config-if)# 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 bvi

To configure the bridge virtual interface for a bridge group, use the **interface bvi** command in global configuration mode. To remove the bridge virtual interface configuration, use the **no** form of this command. Use this command to enter interface configuration mode so you can configure a management IP address for the bridge group.

interface bvi *bridge_group_number*

no interface bvi *bridge_group_number*

Syntax Description

bridge_group_number	Specifies the bridge group number as an integer between 1 and 100.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

A transparent firewall connects the same network on its inside and outside interfaces. Each pair of interfaces belongs to a bridge group, to which you must assign a management IP address. Each bridge group connects to a separate network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the FWSM, and traffic must exit the FWSM before it is routed by an external router back to another bridge group in the FWSM.

Assign each interface to a bridge group using the **interface vlan** command, and then the **bridge-group** command. Use the **interface bvi** command, and then the **ip address** command to configure the management IP address for the bridge group. The management IP address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, such as system messages or communications with AAA servers. You can also use this address for remote management access.

Examples

The following example assigns VLANs 300 and 301 to bridge group 1, then sets the management address and standby address of bridge group 1:

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
```

```
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

Command	Description
bridge-group	Groups two transparent firewall interfaces into a bridge group.
clear configure interface bvi	Clears the bridge virtual interface configuration.
interface	Configures an interface.
ip address	Sets the management IP address for a bridge group.
show running-config interface bvi	Shows the bridge group interface configuration.

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
3.1(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 FWSM is functioning properly, the FWSM will mark itself as failed and a failover may occur (if the active FWSM 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 set the IP address for an interface (in routed mode) or the management address for a bridge group (transparent mode), use the **ip address** command in interface configuration mode. For routed mode, enter interface configuration mode for the VLAN ID (the **interface** command). For transparent mode, enter interface configuration mode for the bridge group (the **interface bvi** command). 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	Sets the IP address for the interface (routed mode) or the management IP address for the bridge group (transparent mode).
mask	(Optional) Sets the subnet mask for the IP address. If you do not set the mask, the FWSM uses the default mask for the IP address class. Do not assign a host address (/32 or 255.255.255.255) to the transparent firewall. Also, do not use other subnets that contain fewer than 3 host addresses (one each for the upstream router, downstream router, and transparent firewall) such as a /30 subnet (255.255.255.252). The FWSM drops all ARP packets to or from the first and last addresses in a subnet. For example, if you use a /30 subnet and assign a reserved address from that subnet to the upstream router, then the FWSM drops the ARP request from the downstream router to the upstream router.
standby *ip_address*	(Optional) Sets the IP address for the standby unit for failover. The standby IP address must be on the same subnet as the main IP address.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

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

In transparent firewall mode, each pair of interfaces belongs to a bridge group, to which you must assign a management IP address. Each bridge group connects to a separate network. The management IP address is required because the FWSM uses this address as the source address for traffic originating on the FWSM, 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. The FWSM does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

Examples

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

```
hostname(config)# interface vlan 100
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)# interface vlan 200
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
```

The following transparent firewall example assigns VLANs 300 and 301 to bridge group 1, then sets the management address and standby address of bridge group 1:

```
hostname(config)# interface vlan 300
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# bridge-group 1
hostname(config-if)# interface vlan 301
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# bridge-group 1
hostname(config-if)# interface bvi 1
hostname(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

Related Commands

Command	Description
interface bvi	Configures a transparent firewall bridge group.
bridge-group	Assigns an interface to a bridge group.
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 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
3.1(1)	Support for 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 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.

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
1.1(1)	This command was introduced.

Usage Guidelines

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.

Normally, the FWSM only looks at the destination address when determining where to forward the packet. Unicast RPF instructs the FWSM 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 FWSM, the FWSM routing table must include a route back to the source address. See RFC 2267 for more information.

For outside traffic, for example, the FWSM 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 FWSM 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 FWSM drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the FWSM 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.

ip-address

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

ip-address *ip-address*

no ip-address

Syntax Description

ip-address	Specifies the IP address of the FWSM.

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
3.1(1)	This command was introduced.

Examples

The following example enters crypto ca trustpoint configuration mode for trustpoint central, and includes the FWSM 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-privacy

To enable the IP Address Privacy feature, use the **ip-address-privacy** command in sip map configuration mode. To disable IP Address Privacy, use the **no** form of this command.

ip-address-privacy

no ip-address-privacy

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
Sip map configuration	•	•	•	•	—

Command History

Release	Modification
FWSM 3.1	This command was introduced.

Usage Guidelines

When IP Address Privacy is enabled, if any two SIP endpoints participating in an IP phone call or instant messaging session use the same internal firewall interface to contact their SIP proxy server on an external firewall interface, all SIP signaling messages go through the SIP proxy server.

IP Address Privacy can be enabled when SIP over TCP or UDP application inspection is enabled. By default, this feature is disabled. If IP Address Privacy is enabled, the FWSM does not translate internal and external host IP addresses embedded in the TCP or UDP payload of inbound SIP traffic, ignoring translation rules for those IP addresses.

Examples

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

```
hostname(config)# access-list sip-acl permit tcp any any eq 5060
hostname(config)# class-map sip-port
hostname(config-cmap)# match access-list sip-acl
hostname(config-cmap)# sip-map inbound_sip
hostname(config-sip-map)# ip-address-privacy
hostname(config-sip-map)# policy-map S1_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip s1_policy
```

Related Commands

Commands	Description
class-map	Defines the traffic class to which to apply security actions.
inspect sip	Enables SIP application inspection.
policy-map	Associates a class map with specific security actions.
sip-map	Defines a SIP application inspection map.

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.T o 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
3.1(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 FWSM. 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 nbar protocol-tagging (IOS)

If you use Programmable Intelligent Services Accelerator (PISA) integration with the FWSM, then to enable the PISA to tag packets with an application type using GRE, use the **ip nbar protocol-tagging** command in interface configuration mode. To disable tagging, use the **no** form of this command.

Note This feature depends on Cisco IOS Release 12.2(18)ZYA, and will not be supported on the FWSM until the Cisco IOS software is released.

ip nbar protocol-tagging [**vlan-list** *vlan_list*]

no ip nbar protocol-tagging [**vlan-list** *vlan_list*]

Syntax Description

vlan-list *vlan_list*	(Optional) If you want to enable tagging on a trunk port and want to limit tagging to particular VLANs, enter a list of VLANs. By default, all VLANs are tagged. The *vlan_list* can be one or more VLANs identified in one of the following ways: • A single number (*n*) • A range (*n-x*) Separate numbers or ranges by commas. For example, enter the following numbers: 5,7-10,13,45-100

Defaults

No default behavior or values.

Command Modes

Interface configuration.

Command History

Release	Modification
12.2(18)ZYA	This command was introduced.

Usage Guidelines

Before you enable protocol tagging, you must enable classification using the **ip nbar protocol-discovery** command. See the Cisco IOS documentation for more information about NBAR classification.

The PISA on the switch supervisor can quickly determine the application type of a given flow by performing deep packet inspection. This determination can be made even if the traffic is not using standard ports. The FWSM can leverage the high-performance deep packet inspection of the PISA card so that it can permit or deny traffic based on the application type. Unlike the FWSM inspection feature, which passes through the control plane path, traffic that the PISA tags can pass through the FWSM accelerated path. Another benefit of FWSM and PISA integration is to consolidate your security configuration on a single FWSM instead of having to configure multiple upstream switches with PISAs installed.

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

After the PISA identifies the application used by a given traffic flow, it encapsulates all packets using GRE and includes a tag informing the FWSM of the application type. In addition, an outer IP header almost identical (except for the Layer 4 protocol, which now indicates GRE) to the inner/original IP header is added. The original Layer 2 header is maintained. This preserves the original routing/switching paths for the modified packet. The GRE encapsulation adds 32 bytes (20 bytes for the outer IP header and 12 bytes for the GRE header).

After the FWSM receives the packet and acts on the information, it strips the GRE encapsulation from the packet.

When you configure the FWSM to deny traffic based on the PISA encapsulation, for the VLAN on which that traffic resides, the PISA encapsulates all traffic (including traffic that you did not specify for denial).

The GRE encapsulation increases the packet size slightly, so you should increase the MTU between the PISA and the FWSM according to the Cisco IOS **mtu** and **system jumbomtu** commands.

The GRE encapsulation causes a slight performance impact for PISA traffic sent to the FWSM.

Note Classification (the **ip nbar protocol-discovery** command) and tagging need to be enabled on the same port; for example, you cannot enable classification on an access ports and tagging on a trunk port.

Examples

The following example enables protocol discovery and tagging on an SVI:

```
Router(config)# interface vlan 100
Router(config-if)# ip nbar protocol-discovery
! enables discovery
Router(config-if)# ip nbar protocol-tagging
! enables tagging
Router(config-if)# mtu 9216
! Allows packet sizes up to 9216 bytes without fragmenting
```

The following example enables protocol discovery and tagging on uplink port GigabitEthernet 6/1:

```
Router(config)# interface gigabitethernet 6/1
Router(config-if)# ip nbar protocol-discovery
! Classification
Router(config-if)# ip nbar protocol-tagging vlan-list 100
! Tagging
Router(config-if)# mtu 9216
! Allow packet size up to 9216 bytes without fragmenting
Router(config)# system jumbomtu 9216
! Set global LAN port MTU to 9216 bytes
```

Related Commands

Command	Description
show ip nbar protocol-tagging	Shows tagging configuration information.

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 {**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
3.1(1)	This command was introduced.

Usage Guidelines

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

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 FWSM before connecting.

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-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
3.1(1)	This command was introduced.

Usage Guidelines

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

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 FWSM 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 FWSM 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.

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
3.1(1)	This command was introduced.

Usage Guidelines

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

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 FWSM that is running NAT.

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 FWSM 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 FWSM.

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
3.1(1)	This command was introduced.

Usage Guidelines

The **ipv6 access-list** command lets you 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 FWSM 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, see the **access-list extended** command.

The **ipv6 access-list icmp** command is used to filter ICMPv6 messages that pass through the FWSM.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 FWSM.
object-group	Creates an object group (addresses, ICMP types, and services).

ipv6 access-list remark

To add a remark to an IPv6 access list, use the **ipv6 access-list remark** command in global configuration mode. To delete the remark, use the **no** form of this command.

ipv6 access-list *id* [**line** *line-num*] **remark** *text*

no ipv6 access-list *id* [**line** *line-num*] **remark** [*text*]

Syntax Description

id	The name of an IPv6 access list.
line *line-num*	(Optional) The line number at which to insert the remark.
remark text	The text of the remark.

Defaults

No default behavior or values.

Command Modes

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

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

Command History

Release	Modification
3.1(1)	This command was introduced.

Usage Guidelines

The remark text can be up to 100 characters in length, including spaces and punctuation. If you enter more than 100 characters, the remark is truncated at the 100th character. The remark text must contain at least 1 non-space character; you cannot enter an empty remark. You can enter more than one remark for each access list.

You cannot use the **access-group** command on an ACL that includes a remark only.

Examples

The following example shows how to specify the text of the remark to add before or after an **ipv6 access-list** command:

```
hostname(config)# ipv6 access-list example remark this access list should not be used
```

Related Commands

Command	Description
access-group	Binds an access list to an interface.
clear configure ipv6 access-list	Clears the IPv6 access lists from the running configuration.
ipv6 access-list	Adds an IPv6 access list to the configuration.
show ipv6 access-list	Displays the IPv6 access lists.
show running-config ipv6	Displays the **ipv6** commands in the running configuration.

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
3.1(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 Vlan101
hostname(config-subif)# ipv6 address 3ffe:c00:0:1::576/64
```

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

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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 Vlan101
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 Vlan101
hostname(config-subif)# 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
3.1(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 Vlan101
hostname(config-subif)# 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: • echo • echo-reply • membership-query • membership-reduction • membership-report • neighbor-advertisement • neighbor-redirect • neighbor-solicitation • destination-unreachable • packet-too-big • parameter-problem • router-advertisement • router-renumbering • router-solicitation • time-exceeded • unreachable
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
3.1(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 FWSM 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 FWSM 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
```

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
3.1(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:

```
%fwsm-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:

```
%fwsm-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 Vlan101
hostname(config-subif)# ipv6 nd dad attempts 5
```

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

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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
3.1(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 Vlan101:

```
hostname(config)# interface Vlan101
hostname(config-subif)# 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:

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

Command History

Release	Modification
3.1(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 Vlan101
hostname(config-subif)# 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
3.1(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 FWSM 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 Vlan101
hostname(config-subif)# 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 FWSM as a default router on this interface. Valid values range from 0 to 9000 seconds. The default is 1800 seconds. 0 indicates that the FWSM 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
3.1(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 FWSM as a default router on this interface.

Setting the value to a non-zero value to indicates that the FWSM 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 FWSM 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 Vlan101
hostname(config-subif)# 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
3.1(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 Vlan101
hostname(config-subif)# 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
3.1(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 Vlan101
hostname(config-subif)# 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
3.1(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
3.1(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
3.1(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
3.1(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 FWSM, 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
1.1(1)	Support for this command was introduced on the FWSM.

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
1.1(1)	This command was introduced.

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.
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
1.1(1)	This command was introduced.

Usage Guidelines

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

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 named 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-ipsec)# isakmp keepalive threshold 15 retry 10
```

Related Commands

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

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
1.1(1)	This command was introduced.

Usage Guidelines

If you specify RSA signatures, you must configure the FWSM 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 FWSM 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
1.1(1)	This command was introduced.

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.

[no] isakmp policy *priority* **group** {**1** | **2** | **5** | **7**}

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
1.1(1)	This command was introduced.

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-if)# 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
1.1(1)	This command was introduced.

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. To reset the security association lifetime to the default value of 86,400 seconds (one day), use the **no** form of this command .

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
1.1(1)	This command was introduced.

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 FWSM 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 FWSM, 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 FWSM, 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
3.1(1)	This command was introduced.

Examples

The following example, entered in global configuration mode, tells the FWSM 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
CA certificate map configuration	•	•	•	•	—

Command History

Release	Modification
3.1(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.