

# int – ipu


- integrity, on page 3
- intercept-dhcp, on page 5
- interface (global), on page 6
- interface (vpn load-balancing), on page 9
- interface bvi, on page 11
- interface loopback, on page 14
- interface-policy, on page 16
- interface port-channel, on page 18
- interface redundant, on page 20
- interface tunnel, on page 22
- interface vlan, on page 23
- interface vni, on page 26
- interim-accounting-update, on page 28
- internal-password, on page 30
- internal-port, on page 32
- internal-segment-id, on page 34
- interval maximum, on page 36
- invalid-ack, on page 38
- ip address, on page 40
- ip address dhcp, on page 43
- ip address pppoe, on page 45
- ip-address-privacy, on page 47
- ip audit attack, on page 48
- ip audit info, on page 50
- ip audit interface, on page 52
- ip audit name, on page 54
- ip audit signature, on page 56
- ip-client, on page 62
- ip-comp, on page 63
- ip local pool, on page 65
- ip unnumbered, on page 67
- ip-phone-bypass, on page 68
- ips, on page 70

- ipsec-udp, on page 73
- ipsec-udp-port, on page 75

# integrity

To specify the ESP integrity algorithm in an IKEv2 security association (SA) for AnyConnect IPsec connections, use the integrity command in IKEv2 policy configuration mode. To remove the command and use the default setting, use the **no** form of this command:

**integrity** { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **null** }
**no integrity** { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **null** }

## Syntax Description

| | |
|---|---|
| **md5** | Specifies the MD5 algorithm for the ESP integrity protection. |
| **null** | Allows an administrator to choose null as the IKEv2 integrity algorithm when AES-GCM is specified as the encryption algorithm. |
| **sha** | (Default) Specifies the Secure Hash Algorithm (SHA) SHA 1, defined in the U.S. Federal Information Processing Standard (FIPS), for ESP integrity protection. |
| sha256 | Specifies the Secure Hash Algorithm SHA 2 with the 256-bit digest. |
| **sha384** | Specifies the Secure Hash Algorithm SHA 2 with the 384-bit digest. |
| **sha512** | Specifies the Secure Hash Algorithm SHA 2 with the 512-bit digest. |

## Command Default

The default is **sha (**SHA 1 algorithm).

## Usage Guidelines

An IKEv2 SA is a key used in phase 1 to enable IKEv2 peers to communicate securely in phase 2. After entering the crypto ikev2 policy command, use the **integrity** command to set the integrity algorithm for the ESP protocol.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 8.4(1) | This command was added. |
| 8.4(2) | The sha256, sha384, and sha512 keywords were added for SHA 2 support. |
| 9.0(1) | The null option as an IKEv2 integrity algorithm was added. |

## Examples

The following example enters IKEv2 policy configuration mode and sets the integrity algorithm to MD5:

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5
```

## Related Commands

| Command | Description |
|---|---|
| encryption | Specifies the encryption algorithm in an IKEv2 SA for AnyConnect IPsec connections. |
| group | Specifies the Diffie-Hellman group in an IKEv2 SA for AnyConnect IPsec connections. |
| lifetime | Specifies the SA lifetime for the IKEv2 SA for AnyConnect IPsec connections. |
| **prf** | Specifies the pseudo-random function in an IKEv2 SA for AnyConnect IPsec connections. |

# intercept-dhcp

To enable DHCP Intercept, use the **intercept-dhcp enable** command in group-policy configuration mode. To remove the **intercept-dhcp** attribute from the running configuration and allow the users to inherit a DHCP Intercept configuration from the default or other group policy, use the **no** form of this command.

**intercept-dhcp** *netmask* { **enable** | **disable** }
**no intercept-dhcp**

## Syntax Description

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

## Command Default

DHCP Intercept is disabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Global-policy configuration | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

To disable DHCP Intercept, use the **intercept-dhcp disable** command.

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

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

## Examples

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

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

# interface (global)

To configure an interface and enter interface configuration mode, use the **interface** command in global configuration mode. To remove a subinterface, use the **no** form of this command; you cannot remove a physical interface or a mapped interface.

For physical interfaces (for all models except the ASASM):

**interface** *physical_interface*
For subinterfaces (not available for the ASA 5505 or the ASASM, or for the Management interface on the ASA 5506-X through ASA 5555-X):

**interface** { *physical_interface* | **redundant** *number* | **port-channel** *number* } **.** *subinterface*
**no interface** { *physical_interface* | **redundant** *number* | **port-channel** *number* } **.** *subinterface*

For multiple context mode when a mapped name is assigned:

**interface** *mapped_name*

## Syntax Description

| | |
|---|---|
| *mapped_name* | In multiple context mode, specifies the mapped name if it was assigned using the **allocate-interface** command. |
| *physical_interface* | Specifies the physical interface type, slot, and port number as *type*[*slot*/]*port*. A space between the type and slot/port is optional.<br>The physical interface types include the following:<br>• **ethernet**<br>• gigabitethernet<br>• **tengigabitethernet**<br>• **management**<br>Enter the type followed by slot/port, for example, **gigabitethernet 0/1**.<br>The management interface is meant for management traffic only. You can, however, use it for through traffic if desired, depending on your model (see the **management-only** command).<br>See the hardware documentation that came with your model to identify the interface type, slot, and port number. |
| **subinterface** | Specifies an integer between 1 and 4294967293 designating a logical subinterface. The maximum number of subinterfaces varies depending on your ASA model. Subinterfaces are not available for the ASA 5505, ASASM, or for the management interface on the ASA 5512-X through ASA 5555-X. See the configuration guide for the maximum subinterfaces (or VLANs) per platform. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. |

## Command Default

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

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

The default state of an interface depends on the type and the context mode:

- Multiple context mode, context—All allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.
- Single mode or multiple context mode, system—Interfaces have the following default states:
  - Physical interfaces—Disabled.
  - Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Global Configuration | • Yes | • Yes | • Yes | • Yes | • Yes |

## Command History

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

## Usage Guidelines

In interface configuration mode, you can configure hardware settings (for physical interfaces), assign a name, assign a VLAN, assign an IP address, and configure many other settings, depending on the type of interface and the security context mode.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For subinterfaces, also configure the **vlan** command.

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

The Management 0/0 interface on the ASA 5512-X through ASA 5555-X has the following characteristics:

- No through traffic support
- No subinterface support
- No priority queue support
- No multicast MAC support
- The IPS SSP software module shares the Management 0/0 interface. Separate MAC addresses and IP addresses are supported for the ASA and IPS module. You must perform configuration of the IPS IP

address within the IPS operating system. However, physical characteristics (such as enabling the interface) are configured on the ASA.

## Examples

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

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

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

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

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

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

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

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

## Related Commands

| Command | Description |
|---|---|
| **allocate-interface** | Assigns interfaces and subinterfaces to a security context. |
| **member-interface** | Assigns interfaces to a redundant interface. |
| **clear interface** | Clears counters for the **show interface** command. |
| **show interface** | Displays the runtime status and statistics of interfaces. |
| **vlan** | Assigns a VLAN to a subinterface. |

# interface (vpn load-balancing)

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

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

## Syntax Description

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

## Command Default

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

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| vpn load-balancing | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

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

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

## Examples

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

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
```

```
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# no
 interface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

ciscoasa(config-load-balancing)# **participate**

## Related Commands

| Command | Description |
|---|---|
| **vpn load-balancing** | Enters vpn load-balancing configuration mode. |

# interface bvi

To configure the bridge virtual interface (BVI) for a bridge group, use the **interface bvi** command in global configuration mode. To remove the BVI configuration, use the **no** form of this command.

**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; for 9.3(1) and later, the range is increased to between 1 and 250. |

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 8.4(1) | This command was added. |
| 9.3(1) | The number range was increased to between 1 and 250 to support 250 BVIs. |
| 9.6(2) | The maximum interfaces per bridge group was increased from 4 to 64. |

## Usage Guidelines

Use this command to enter interface configuration mode so you can configure a management IP address for the bridge group. If you do not want the overhead of security contexts, or want to maximize your use of security contexts, you can group interfaces together in a bridge group, and then configure multiple bridge groups, one for each network. Bridge group traffic is isolated from other bridge groups; traffic is not routed to another bridge group within the ASA, and traffic must exit the ASA before it is routed by an external router back to another bridge group in the ASA. Although the bridging functions are separate for each bridge group, many other functions are shared between all bridge groups. For example, all bridge groups share a syslog server or AAA server configuration. For complete security policy separation, use security contexts with one bridge group in each context. At least one bridge group is required per context or in single mode.

Each bridge group requires a management IP address. The ASA uses this IP address as the source address for packets originating from the bridge group. The management IP address must be on the same subnet as the connected network. For IPv4 traffic, the management IP address is required to pass any traffic. For IPv6 traffic, you must, at a minimum, configure the link-local addresses to pass traffic, but a global management address is recommended for full functionality, including remote management and other management operations.

For another method of management, you can configure the Management interface, separate from any bridge groups.

For 9.2 and earlier, You can configure up to 8 bridge groups in single mode or per context in multiple mode; for 9.3(1) and later, you can configure up to 250 bridge groups. Each bridge group can include up to 4 interfaces. In 9.6(2) and later, you can add up to 64 interfaces to a bridge group. You cannot assign the same interface to more than one bridge group. Note that you must use at least 1 bridge group; data interfaces must belong to a bridge group.

**Note** Although you can configure multiple bridge groups on the ASA 5505, the restriction of 2 data interfaces in transparent mode on the ASA 5505 means you can only effectively use 1 bridge group.

**Note** For a separate management interface, a non-configurable bridge group (ID 301) is automatically added to your configuration. This bridge group is not included in the bridge group limit.

**Note** The ASA does not support traffic on secondary networks; only traffic on the same network as the management IP address is supported.

## Examples

The following example includes two bridge groups of three interfaces each, plus a management-only interface:

```
interface gigabitethernet 0/0
nameif inside
security-level 100
bridge-group 1
no shutdown
interface gigabitethernet 0/1
nameif outside
security-level 0
bridge-group 1
no shutdown
interface gigabitethernet 0/2
nameif dmz
security-level 50
bridge-group 1
no shutdown
interface bvi 1
ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
interface gigabitethernet 1/0
nameif inside
security-level 100
bridge-group 2
no shutdown
interface gigabitethernet 1/1
nameif outside
security-level 0
bridge-group 2
no shutdown
interface gigabitethernet 1/2
```

```
nameif dmz
security-level 50
bridge-group 2
no shutdown
interface bvi 2
ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
interface management 0/0
nameif mgmt
security-level 100
ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
no shutdown
```

## Related Commands

| Command | Description |
|---|---|
| ace/bvi | Clears the bridge virtual interface configuration. |
| **bridge-group** | Groups transparent firewall interfaces into a bridge group. |
| **interface** | Configures an interface. |
| **ip address** | Sets the management IP address for a bridge group. |
| show bridge-group | Shows bridge group information, including member interfaces and IP addresses. |
| show running-config interface bvi | Shows the bridge group interface configuration. |

# interface loopback

To create a loopback interface, use the **interface loopback** command in the global configuration mode. Use the **no** form of the command to remove the loopback interface.

**interface loopback** *number*
**no interface loopback** *number*

## Command Default

No default behavior or values.

## Command Modes

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

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

## Usage Guidelines

A loopback interface is software-only interface that emulates a physical interface. The loopback interface is reachable through multiple physical interfaces. You can only use a loopback interface for to/from the device traffic.

The following features support the loopback interface:

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- Syslog
- Telnet
- VTI source interface

## Command History

| Release | Modification |
|---|---|
| 9.18(2) | This command was added. |
| 9.19(1) | Support for VTI was added. |

| Release | Modification |
|---|---|
| 9.20(1) | Support for DNS, HTTP, and ICMP was added. |

## Examples

The following example creates a new loopback interface:

```
ciscoasa(config)# interface loopback 10
```

## Related Commands

| Command | Description |
|---|---|
| **tunnel source interface** | Specifies the source interface to create a VTI tunnel. |
| **ssh** | Configures SSH for an interface. |
| **logging host** | Specifies the syslog host. |
| **neighbor update-source** | Configures an interface as the source for a BGP-speaking neighbor. |
| **snmp-server host** | Specifies the SNMP server. |
| **telnet** | Configures Telnet for an interface. |

# 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. |

## Command Default

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:

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Failover group Configuration | • Yes | • Yes | — | — | • Yes |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## 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 ASA is functioning correctly, the ASA will mark itself as failed and a failover may occur (if the active ASA 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:

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(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. |

# interface port-channel

To configure an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command in global configuration mode. To remove an EtherChannel interface, use the **no** form of this command.

**interfaceport-channel***number*
**no interface port-channel** *number*

## Syntax Description

*number* Specifies the EtherChannel channel group ID, between 1 and 48. This interface was created automatically when you added an interface to the channel group. If you have not yet added an interface, then this command creates the port-channel interface.

**Note**
You need to add at least one member interface to the port-channel interface before you can configure logical parameters for it, such as a name.

## Command Default

By default, port-channel interfaces are enabled. However, for traffic to pass through the EtherChannel, the channel group physical interfaces must also be enabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Global Configuration | • Yes | • Yes | • Yes | • Yes | • Yes |

## Command History

| Release | Modification |
|---|---|
| 8.4(1) | This command was added. |

## Usage Guidelines

In interface configuration mode, you can assign a name, assign an IP address, and configure many other settings.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**.

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

**Note** This command is not supported on the ASA 5505 or the ASASM. You cannot use interfaces on the 4GE SSM, including the integrated 4GE SSM in slot 1 on the ASA 5550, as part of an EtherChannel.

For more information about interfaces, see the CLI configuration guide.

## Examples

The following example configures three interfaces as part of an EtherChannel. It also sets the system priority to be a higher priority, and GigabitEthernet 0/2 to be a higher priority than the other interfaces in case more than eight interfaces are assigned to the EtherChannel.

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

## Related Commands

| Command | Description |
|---|---|
| channel-group | Adds an interface to an EtherChannel. |
| **interface port-channel** | Configures an EtherChannel. |
| **lacp max-bundle** | Specifies the maximum number of active interfaces allowed in the channel group. |
| **lacp port-priority** | Sets the priority for a physical interface in the channel group. |
| **lacp system-priority** | Sets the LACP system priority. |
| **port-channel load-balance** | Configures the load-balancing algorithm. |
| **port-channel min-bundle** | Specifies the minimum number of active interfaces required for the port-channel interface to become active. |
| **show lacp** | Displays LACP information such as traffic statistics, system identifier and neighbor details. |
| **show port-channel** | Displays EtherChannel information in a detailed and one-line summary form. This command also displays the port and port-channel information. |
| **show port-channel load-balance** | Displays port-channel load-balance information along with the hash result and member interface selected for a given set of parameters. |

# interface redundant

To configure a redundant interface and enter interface configuration mode, use the **interface redundant** command in global configuration mode. To remove a redundant interface, use the **no** form of this command.

**interface redundant** *number*
**no interface redundant** *number*

## Syntax Description

| | |
|---|---|
| *number* | Specifies a logical redundant interface ID, between 1 and 8. A space between **redundant** and the ID is optional. |

## Command Default

By default, redundant interfaces are enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Global Configuration | • Yes | • Yes | • Yes | • Yes | • Yes |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was added. |

## Usage Guidelines

A redundant interface pairs an active and a standby physical interface (see the **member-interface** command). When the active interface fails, the standby interface becomes active and starts passing traffic.

All ASA configuration refers to the logical redundant interface instead of the member physical interfaces.

In interface configuration mode, you can assign a name, assign an IP address, and configure many other settings.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**.

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

**Note** This command is not supported on the ASA 5505 or the ASASM.

For more information about interfaces, see the CLI configuration guide.

## Examples

The following example creates two redundant interfaces:

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

## Related Commands

| Command | Description |
|---|---|
| **clear interface** | Clears counters for the **show interface** command. |
| **debug redundant-interface** | Displays debug messages related to redundant interface events or errors. |
| **interface redundant** | Creates a redundant interface. |
| **member-interface** | Assigns a physical interface to a redundant interface. |
| **redundant-interface** | Changes the active member interface. |
| **show interface** | Displays the runtime status and statistics of interfaces. |

# interface tunnel

To create a new VTI tunnel interface, use the **interface tunnel** command in the Global Configuration mode. Use the no form of the command to remove the VTI tunnel interface.

**interface tunnel** *number*
**no interface tunnel** *number*

## Syntax Description

| | |
|---|---|
| *number* | Assigns a number to the tunnel interface. This can be any value between 0-1024. |

## Command Default

No default behavior or values.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Global Configuration | • Yes | • No | • Yes | • No | • - |

## Command History

| Release | Modification |
|---|---|
| 9.7(1) | We introduced this command and its submodes. |
| 9.16(1) | The number of tunnel interfaces supported was increased from 100 to 1024 per device. |

## Examples

The following example creates a new tunnel interface:

```
ciscoasa(config)# interface tunnel 10
```

## Related Commands

| Command | Description |
|---|---|
| **tunnel source interface** | Specifies the source interface to create a VTI tunnel. |
| **tunnel destination** | Specifies the IP address of the VTI tunnel's destination. |
| **tunnel mode** | Specifies that IPsec is used for tunnel protection. |
| **tunnel protection ipsec** | Specifies the IPsec profile that will be used for tunnel protection. |

# interface vlan

For the ASA 5505 and ASASM, to configure a VLAN interface and enter interface configuration mode, use the **interface vlan** command in global configuration mode. To remove a VLAN interface, use the **no** form of this command.

**interface vlan** *number*
**no interface vlan** *number*

## Syntax Description

*number* Specifies a VLAN ID.

For the ASA 5505, use an ID between 1 and 4090. The VLAN interface ID is enabled by default on VLAN 1.

For the ASASM, use an ID between 2 to 1000 and from 1025 to 4094.

## Command Default

By default, VLAN interfaces are enabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Global Configuration | • Yes | • Yes | • Yes | • Yes | • Yes |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was added. |
| 8.4(1) | ASASM support was added. |

## Usage Guidelines

For the ASASM, you can add any VLAN ID to the configuration, but only VLANs that are assigned to the ASA by the switch can pass traffic. To view all VLANs assigned to the ASA, use the **show vlan** command. If you add an interface for a VLAN that is not yet assigned to the ASA by the switch, the interface will be in the down state. When you assign the VLAN to the ASA, the interface changes to an up state. See the **show interface** command for more information about interface states.

In interface configuration mode, you can assign a name, assign an IP address, and configure many other settings.

For an enabled interface to pass traffic, configure the following interface configuration mode commands: **nameif**, and, for routed mode, **ip address**. For the ASA 5505 switch physical interfaces, assign the physical interface to the VLAN interface using the **switchport access vlan** command.

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

For more information about interfaces, see the CLI configuration guide.

## Examples

The following example configures three VLAN interfaces. The third home interface cannot forward traffic to the work interface.

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
```

The following example configures five VLAN interfaces, including the failover interface, which is configured separately using the **failover lan** command:

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
```

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
255.255.255.0
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

## Related Commands

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

# interface vni

To configure a VXLAN Network Identifier (VNI) interface and enter interface configuration mode, use the **interface vni** command in global configuration mode. To remove a VNI interface, use the **no** form of this command.

**interface vni** *number*
**no interface vni** *number*

## Syntax Description

| | |
|---|---|
| *number* | Sets the ID between 1 and 10000. This ID is only an internal interface identifier. |

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 9.4(1) | This command was added. |

## Usage Guidelines

You must associate a VNI interface with a VTEP source interface using the **vtep-nve** command. You must also set the VXLAN **segment-id**.

## Examples

The following example configures the GigabitEthernet 1/1 interface as the VTEP source interface, and associates the VNI 1 interface wth it:

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

## Related Commands

| Command | Description |
|---|---|
| **debug vxlan** | Debugs VXLAN traffic. |
| **default-mcast-group** | Specifies a default multicast group for all VNI interfaces associated with the VTEP source interface. |
| **encapsulation vxlan** | Sets the NVE instance to VXLAN encapsulation. |
| **inspect vxlan** | Enforces compliance with the standard VXLAN header format. |
| **interface vni** | Creates the VNI interface for VXLAN tagging. |
| **mcast-group** | Sets the multicast group address for the VNI interface. |
| **nve** | Specifies the Network Virtualization Endpoint instance. |
| nve-only | Specifies that the VXLAN source interface is NVE-only. |
| **peer ip** | Manually specifies the peer VTEP IP address. |
| **segment-id** | Specifies the VXLAN segment ID for a VNI interface. |
| **show arp vtep-mapping** | Displays MAC addresses cached on the VNI interface for IP addresses located in the remote segment domain and the remote VTEP IP addresses. |
| **show interface vni** | Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with. |
| **show mac-address-table vtep-mapping** | Displays the Layer 2 forwarding table (MAC address table) on the VNI interface with the remote VTEP IP addresses. |
| **show nve** | Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface. |
| **show vni vlan-mapping** | Shows the mapping between VNI segment IDs and VLAN interfaces or physical interfaces in transparent mode. |
| **source-interface** | Specifies the VTEP source interface. |
| **vtep-nve** | Associates a VNI interface with the VTEP source interface. |
| **vxlan port** | Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789. |

# interim-accounting-update

To enable the generation of RADIUS interim-accounting-update messages for the AAA server group, use the **interim-accounting-update** command in aaa-server group configuration mode. To disable interim-accounting-update messages, use the **no** form of this command.

**interim-accounting-update** [ **periodic** [ *hours* ] ]
**no interim-accounting-update** [ **periodic** [ *hours* ] ]

## Syntax Description

| | |
|---|---|
| **periodic** [*hours*] | (Optional) Enables the periodic generation and transmission of accounting records for every VPN session that is configured to send accounting records to the server group in question. You can optionally include the interval, in hours, for sending these updates. The default is 24 hours, the range is 1 to 120.<br><br>Use this option for a server group configured for ISE Change of Authentication. |

## Command Default

By default interim-accounting-update is not enabled.

## 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 |
| aaa-server group configuration | • Yes | • Yes | • Yes | • Yes | — |

## Command History

| Release | Modification |
|---|---|
| 9.2(1) | The **periodic** keyword was added. |

## Usage Guidelines

If you use this command without the **periodic** keyword, the ASA sends interim-accounting-update messages only when a VPN tunnel connection is added to a clientless VPN session. When this happens the accounting update is generated in order to inform the RADIUS server of the newly assigned IP address.

If you are using the server group to configure ISE Change of Authorization for a remote access VPN, add the **periodic** keyword. Period reporting includes AnyConnect connections as well as clientless sessions.

ISE maintains a directory of active sessions based on the accounting records that it receives from NAS devices like the ASA. However, if ISE does not receive any indication that the session is still active accounting message or posture transactions) for a period of 5 days, it will remove the session record from its database. To ensure that long-lived VPN connections are not removed, configure the group to send periodic interim-accounting-update messages to ISE for all active sessions.

## Examples

The following example shows how to configure an ISE server group for dynamic authorization (CoA) updates and hourly periodic accounting. Included is the tunnel group configuration that configures password authentication with ISE.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

The following example shows how to configure a tunnel group for local certificate validation and authorization with ISE. In this case, you include the **authorize-only** command in the server group configuration, because the server group will not be used for authentication.

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

## Related Commands

| Command | Description |
|---|---|
| **authorize-only** | Enables authorize-only mode for the RADIUS server group. |
| **dynamic-authorization** | Enables dynamic authorization for the RADIUS server group. |

# internal-password

To display an additional password field on the clientless SSL VPN portal page, use the **internal-password** command in webvpn configuration mode. This additional password is used by the ASA to authenticate users to file servers for whom SSO is allowed.

To disable the ability to use an internal password, use the **no** version of the command.

**internal-passwordenable**
**no internal password**

## Syntax Description

| | |
|---|---|
| **enable** | Enables use of an internal password. |

## Command Default

The default is disabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Webvpn configuration | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 8.0(2) | This command was added. |

## Usage Guidelines

If enabled, end users type a second password when logging in to a clientless SSL VPN session. The clientless SSL VPN server sends an SSO authentication request, including the username and password, to the authenticating server using HTTPS. If the authenticating server approves the authentication request, it returns an SSO authentication cookie to the clientless SSL VPN server. This cookie is kept on the ASA on behalf of the user and used to authenticate the user to secure websites within the domain protected by the SSO server.

The internal password feature is useful if you require that the internal password be different from the SSL VPN password. In particular, you can use one-time passwords for authentication to the ASA, and another password for internal sites.

## Examples

The following example shows how to enable the internal password:

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 internal password enable
ciscoasa(config-webvpn)#
```

**Related Commands**

| Command | Description |
|---|---|
| webvpn | Enters webvpn configuration mode, which lets you configure attributes for clientless SSL VPN connections. |

# internal-port

To specify the VXLAN internal port for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **internal-port** command in interface configuration mode. To remove the port, use the **no** form of this command.

**internal-port** *port*
**no internal-port** *port*

## Syntax Description

| | |
|---|---|
| *port* | Sets the port between 1024 and 65535. |

## Command Default

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 |
| Interface configuration | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 9.19(1) | This command was added. |

## Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

## Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

**Related Commands**

| Command | Description |
|---|---|
| **debug vxlan** | Debugs VXLAN traffic. |
| **encapsulation vxlan** | Sets the NVE instance to VXLAN encapsulation. |
| **external-port** | Sets the external VXLAN port. |
| **external-segment-id** | Specifies the VXLAN external segment ID for a VNI interface. |
| **inspect vxlan** | Enforces compliance with the standard VXLAN header format. |
| **interface vni** | Creates the VNI interface for VXLAN tagging. |
| **internal-segment-id** | Specifies the VXLAN internal segment ID for a VNI interface. |
| **nve** | Specifies the Network Virtualization Endpoint instance. |
| **peer ip** | Manually specifies the peer VTEP IP address. |
| **proxy paired** | Sets the interface to paired proxy mode. |
| **show interface vni** | Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with. |
| **show nve** | Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface. |
| **source-interface** | Specifies the VTEP source interface. |
| **vtep-nve** | Associates a VNI interface with the VTEP source interface. |
| **vxlan port** | Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789. |

# internal-segment-id

To specify the VXLAN internal segment ID for a VNI interface for the ASA virtual on Azure for the Azure Gateway Load Balancer (GWLB), use the **internal-segment-id** command in interface configuration mode. To remove the ID, use the **no** form of this command.

**internal-segment-id** *id*
**no internal-segment-id** *id*

## Syntax Description

| | |
|---|---|
| *id* | Sets the ID between 1 and 16777215. |

## Command Default

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 |
| Interface configuration | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 9.19(1) | This command was added. |

## Usage Guidelines

In an Azure service chain, ASA virtuals act as a transparent gateway that can intercept packets between the internet and the customer service. The ASA virtual defines an external interface and an internal interface on a single NIC by utilizing VXLAN segments in a paired proxy.

## Examples

The following example configures the VNI 1 interface for Azure GWLB:

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

**Related Commands**

| Command | Description |
|---|---|
| **debug vxlan** | Debugs VXLAN traffic. |
| **encapsulation vxlan** | Sets the NVE instance to VXLAN encapsulation. |
| **external-port** | Sets the external VXLAN port. |
| **external-segment-id** | Specifies the VXLAN external segment ID for a VNI interface. |
| **inspect vxlan** | Enforces compliance with the standard VXLAN header format. |
| **interface vni** | Creates the VNI interface for VXLAN tagging. |
| **internal-port** | Sets the internal VXLAN port. |
| **nve** | Specifies the Network Virtualization Endpoint instance. |
| **peer ip** | Manually specifies the peer VTEP IP address. |
| **proxy paired** | Sets the interface to paired proxy mode. |
| **show interface vni** | Shows the parameters, status and statistics of a VNI interface, status of its bridged interface (if configured), and NVE interface it is associated with. |
| **show nve** | Shows the parameters, status and statistics of a NVE interface, status of its carrier interface (source interface), IP address of the carrier interface, VNIs that use this NVE as the VXLAN VTEP, and peer VTEP IP addresses associated with this NVE interface. |
| **source-interface** | Specifies the VTEP source interface. |
| **vtep-nve** | Associates a VNI interface with the VTEP source interface. |
| **vxlan port** | Sets the VXLAN UDP port. By default, the VTEP source interface accepts VXLAN traffic to UDP port 4789. |

# interval maximum

To configure the maximum interval between update attempts by a DDNS update method, use the **interval** command in DDNS-update-method mode. To remove an interval for a DDNS update method from the running configuration, use the **no** form of this command.

**interval maximum** *days hours minutes seconds*
**no interval maximum** *days hours minutes seconds*

## Syntax Description

| | |
|---|---|
| days | Specifies the number of days between update attempts with a range of 0 to 364. |
| hours | Specifies the number of hours between update attempts with a range of 0 to 23. |
| minutes | Specifies the number of minutes between update attempts with a range of 0 to 59. |
| seconds | Specifies the number of seconds between update attempts with a range of 0 to 59. |

## Command Default

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 |
| Ddns-update-method configuration | • Yes | — | • Yes | • Yes | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was added. |

## Usage Guidelines

The days, hours, minutes, and seconds are added together to arrive at the total interval.

## Examples

The following example configures a method called ddns-2 to attempt an update every 3 minutes and 15 seconds:

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

## Related Commands

| Command | Description |
|---|---|
| **ddns** | Specifies a DDNS update method type for a created DDNS method. |

| Command | Description |
|---|---|
| **ddns update** | Associates a DDNS update method with an ASA interface or a DDNS update hostname. |
| ddns update method | Creates a method for dynamically updating DNS resource records. |
| **dhcp-client update dns** | Configures the update parameters that the DHCP client passes to the DHCP server. |
| dhcpd update dns | Enables a DHCP server to perform DDNS updates. |

# invalid-ack

To set the action for packets with an invalid ACK, use the **invalid-ack** command in tcp-map configuration mode. To set the value back to the default, use the **no** form of this command. This command is part of the TCP normalization policy enabled using the **set connection advanced-options** command.

**invalid-ack** { **allow** | **drop** }
**no invalid-ack**

## Syntax Description

| | |
|---|---|
| **allow** | Allows packets with an invalid ACK. |
| **drop** | Drops packets with an invalid ACK. |

## Command Default

The default action is to drop packets with an invalid ACK.

## 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 |
| Tcp-map configuration | • Yes | • Yes | • Yes | • Yes | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(4)/8.0(4) | This command was added. |

## Usage Guidelines

To enable TCP normalization, use the Modular Policy Framework:

1. **tcp-map**—Identifies the TCP normalization actions.
   a. **invalid-ack**—In tcp-map configuration mode, you can enter the **invalid-ack** command and many others.
2. **class-map**—Identify the traffic on which you want to perform TCP normalization.
3. **policy-map**—Identify the actions associated with each class map.
   a. **class**—Identify the class map on which you want to perform actions.
   b. **set connection advanced-options**—Identify the TCP map you created.
4. **service-policy**—Assigns the policy map to an interface or globally.

You might see invalid ACKs in the following instances:

- In the TCP connection SYN-ACK-received status, if the ACK number of a received TCP packet is not exactly the same as the sequence number of the next TCP packet sending out, it is an invalid ACK.
- Whenever the ACK number of a received TCP packet is greater than the sequence number of the next TCP packet sending out, it is an invalid ACK.



**Note** TCP packets with an invalid ACK are automatically allowed for WAAS connections.

## Examples

The following example sets the ASA to allow packets with an invalid ACK:

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Identifies traffic for a service policy. |
| **policy-map** | Identifies actions to apply to traffic in a service policy. |
| **set connection advanced-options** | Enables TCP normalization. |
| service-policy | Applies a service policy to interface(s). |
| show running-config tcp-map | Shows the TCP map configuration. |
| **tcp-map** | Creates a TCP map and allows access to tcp-map configuration mode. |

# ip address

To set the IP address for an interface (in routed mode) or for the bridge virtual interface (BVI) (routed or transparent mode), use the **ip address** command in interface configuration mode. To remove the IP address, use the **no** form of this command.

**ip address** *ip_address* [ *mask* ] **standby** *ip_address* | **cluster-pool** *poolname* ]
**no ip address** [ *ip_address* ]

## Syntax Description

| | |
|---|---|
| **cluster-pool** *poolname* | (Optional) For ASA clustering, sets the cluster pool of addresses defined by the **ip local pool** command. The main cluster IP address defined by the *ip_address* argument belongs to the current master unit only. Each cluster member receives a local IP address from this pool.<br><br>You cannot determine the exact address assigned to each unit in advance; to see the address used on each unit, enter the **show ip local pool** *poolname* command. Each cluster member is assigned a member ID when it joins the cluster. The ID determines the local IP used from the pool. |
| *ip_address* | The IP address for the interface. |
| *mask* | (Optional) The subnet mask for the IP address. If you do not set the mask, the ASA uses the default mask for the IP address class. |
| **standby** *ip_address* | (Optional) For failover, sets the IP address for the standby unit. |

## Command Default

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 |
| Interface Configuration | • Yes | • Yes | • Yes | • Yes | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | For routed mode, this command was changed from a global configuration command to an interface configuration mode command. |
| 8.4(1) | For transparent mode, bridge groups were added. You now set the IP address for the BVI, and not globally. |
| 9.0(1) | The **cluster-pool** keyword was added to support ASA clustering. |

| Release | Modification |
|---|---|
| 9.7(1) | For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. |

## Usage Guidelines

This command also sets the standby address for failover.

### Multiple Context Mode 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.

### Transparent Firewall Guidelines

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

### Failover Guidelines

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

### ASA Clustering Guidelines

You can only set the cluster pool for an individual interface after you configure the cluster interface mode to be individual (**cluster-interface mode individual** command). The only exception is for the management-only interface(s):

- You can always configure the management-only interface as an individual interface, even in spanned EtherChannel mode. The management interface can be an individual interface even in transparent firewall mode.
- In spanned EtherChannel mode, if you configure the management interface as an individual interface, you cannot enable dynamic routing for the management interface. You must use a static route.

### /31 Subnet Guidelines

For routed interfaces, you can configure an IP address on a 31-bit subnet for point-to-point connections. The 31-bit subnet includes only 2 addresses; normally, the first and last address in the subnet is reserved for the network and broadcast, so a 2-address subnet is not usable. However, if you have a point-to-point connection and do not need network or broadcast addresses, a 31-bit subnet is a useful way to preserve addresses in IPv4. For example, the failover link between 2 ASAs only requires 2 addresses; any packet that is transmitted by one end of the link is always received by the other, and broadcasting is unnecessary. You can also have a directly-connected management station running SNMP or Syslog.

- 31-Bit Subnet and Clustering—You can use a 31-bit subnet mask for Spanned EtherChannels. Individual interfaces (including the Management IP address in Spanned EtherChannel mode) do not support a 31-bit subnet. You also cannot use the 31-bit subnet for the Cluster Control Link.
- 31-Bit Subnet and Failover—For failover, when you use a 31-bit subnet for the ASA interface IP address, you cannot configure a standby IP address for the interface because there are not enough addresses. Normally, an interface for failover should have a standby IP address so the active unit can perform

interface tests to ensure standby interface health. Without a standby IP address, the ASA cannot perform any network tests; only the link state can be tracked. For the failover and optional separate state link, which are point-to-point connections, you can also use a 31-bit subnet.

- 31-Bit Subnet and Management—If you have a directly-connected management station, you can use a point-to-point connection for SSH or HTTP on the ASA, or for SNMP or Syslog on the management station.
- 31-Bit Subnet Unsupported Features—The following features do not support the 31-Bit subnet:
  - BVI interfaces for bridge groups— The bridge group requires at least 3 host addresses: the BVI, and two hosts connected to two bridge group member interfaces. you must use a /29 subnet or smaller.
  - Multicast Routing

## Examples

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

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

The following example sets the management address and standby address of bridge group 1:

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

## Related Commands

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

# ip address dhcp

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

**ip address dhcp** [ **setroute** ]
**no ip address dhcp**

## Syntax Description

| | |
|---|---|
| **setroute** | (Optional) Allows the ASA to use the default route supplied by the DHCP server. |

## Command Default

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 |
| Interface configuration | • Yes | — | • Yes | • Yes | — |

## Command History

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

## Usage Guidelines

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

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

**Note** The ASA rejects any leases that have a timeout of less than 32 seconds.

## Examples

The following example enables DHCP on the Gigabitethernet0/1 interface:

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

## Related Commands

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

# ip address pppoe

To enable PPPoE, use the **ip address pppoe** command in interface configuration mode. To disable PPPoE, use the **no** form of this command.

**ip address** [ *ip_address* [ *mask* ] ] **pppoe** [ **setroute** ]
**no ip address** [ *ip_address* [ *mask* ] ] **pppoe**

## Syntax Description

| | |
|---|---|
| *ip_address* | Manually sets the IP address instead of receiving an address from the PPPoE server. |
| *mask* | Specifies the subnet mask for the IP address. If you do not set the mask, the ASA uses the default mask for the IP address class. |
| **setroute** | Lets the ASA use the default route supplied by the PPPoE server. If the PPPoE server does not send a default route, the ASA creates a default route with the address of the access concentrator as the gateway. |

## Command Default

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 |
| Interface configuration | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was added. |

## Usage Guidelines

PPPoE combines two widely accepted standards, Ethernet and PPP, to provide an authenticated method of assigning IP addresses to client systems. ISPs deploy PPPoE because it supports high-speed broadband access using their existing remote access infrastructure and because it is easier for customers to use.

Before you set the IP address using PPPoE, configure the **vpdn** commands to set the username, password, and authentication protocol. If you enable this command on more than one interface, for example for a backup link to your ISP, then you can assign each interface to a different VPDN group if necessary using the pppoe client vpdn group command.

The maximum transmission unit (MTU) size is automatically set to 1492 bytes, which is the correct value to allow PPPoE transmission within an Ethernet frame.

Reenter this command to reset and restart the PPPoE session.

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

## Examples

The following example enables PPPoE on the Gigabitethernet 0/1 interface:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

The following example manually sets the IP address for a PPPoE interface:

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
ciscoasa(config-if)# no shutdown
```

## Related Commands

| Command | Description |
|---|---|
| **interface** | Configures an interface and enters interface configuration mode. |
| ip address | Sets the IP address for an interface. |
| pppoe client vpdn group | Assigns this interface to a particular VPDN group. |
| show ip address pppoe | Shows the IP address obtained from the PPPoE server. |
| vpdn group | Creates a vpdn group and configures PPPoE client settings. |

# ip-address-privacy

To enable IP address privacy, use the **ip-address-privacy** command in parameters configuration mode. Parameters configuration mode is accessible from policy map configuration mode. To disable this feature, use the **no** form of this command.

**ip-address-privacy**
**no ip-address-privacy**

## Syntax Description

This command has no arguments or keywords.

## Command Default

This command is disabled by default.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Parameters Configuration | • Yes | • Yes | • Yes | • Yes | — |

## Command History

| Release | Modification |
|---|---|
| 7.2(1) | This command was added. |

## Examples

The following example shows how to enable IP address privacy over SIP in a SIP inspection policy map:

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ip-address-privacy
```

## Related Commands

| Command | Description |
|---|---|
| **policy-map type inspect** | Creates an inspection policy map. |
| **show running-config policy-map** | Display all current policy map configurations. |

# ip audit attack

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

**ip audit attack** [ **action** [ **alarm** ] [ **drop** ] [ **reset** ] ]
**no ip audit attack**

## Syntax Description

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

## Command Default

The default action is to send and alarm.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

You can specify multiple actions, or no actions. You can override the action you set with this command when you configure an audit policy using the **ip audit name** command. If you do not specify the action in the **ip audit name** command, then the action you set with this command is used.

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

## Examples

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

```
ciscoasa(config)# ip audit attack action alarm reset
ciscoasa(config)# ip audit name insidepolicy attack action alarm
```

```
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

## Related Commands

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

# ip audit info

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

**ip audit info** [ **action** [ **alarm** ] [ **drop** ] [ **reset** ] ]
**no ip audit info**

## Syntax Description

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

## Command Default

The default action is to generate an alarm.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

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

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

## Examples

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

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

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

## Related Commands

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

# ip audit interface

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

**ip audit interface** *interface_name policy_name*
**no ip audit interface** *interface_name policy_name*

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Examples

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

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

## Related Commands

| Command | Description |
|---|---|
| **ip audit attack** | Sets the default actions for packets that match an attack signature. |
| **ip audit info** | Sets the default actions for packets that match an informational signature. |

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

# ip audit name

To create a named audit policy that identifies the actions to take when a packet matches a predefined attack signature or informational signature, use the **ip audit name** command in global configuration mode. To remove the policy, use the **no** form of this command.

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

## Syntax Description

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

## Command Default

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

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

Signatures are activities that match known attack patterns. For example, there are signatures that match DoS attacks. To apply the policy, assign it to an interface using the **ip audit interface** command. You can assign an info policy and an attack policy to each interface.

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

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

## Examples

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

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

## Related Commands

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

# ip audit signature

To disable a signature for an audit policy, use the **ip audit signature** command in global configuration mode. To reenable the signature, use the **no** form of this command.

**ip audit signature** *signature_number* **disable**
**no ip audit signature** *signature_number*

## Syntax Description

| | |
|---|---|
| **disable** | Disables the signature. |
| *signature_number* | Specifies the signature number to disable. See Table 3-1 for a list of supported signatures. |

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

You might want to disable a signature if legitimate traffic continually matches a signature, and you are willing to risk disabling the signature to avoid large numbers of alarms. Table 3-1 lists supported signatures and system message numbers.

***Table 1: Signature IDs and System Message Numbers***

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

| Signature ID | Message Number | Signature Title | Signature Type | Description |
|---|---|---|---|---|
| 1002 | 400002 | IP options-Timestamp | Informational | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp). |
| 1003 | 400003 | IP options-Security | Informational | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options). |
| 1004 | 400004 | IP options-Loose Source Route | Informational | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route). |
| 1005 | 400005 | IP options-SATNET ID | Informational | Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier). |
| 1006 | 400006 | IP options-Strict Source Route | Informational | Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing). |
| 1100 | 400007 | IP Fragment Attack | Attack | Triggers when any IP datagram is received with an offset value less than 5 but greater than 0 indicated in the offset field. |
| 1102 | 400008 | IP Impossible Packet | Attack | Triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack. |
| 1103 | 400009 | IP Overlapping Fragments (Teardrop) | Attack | Triggers when two fragments contained within the same IP datagram have offsets that indicate that they share positioning within the datagram. This could mean that fragment A is being completely overwritten by fragment B, or that fragment A is partially being overwritten by fragment B. Some operating systems do not properly handle fragments that overlap in this manner and may throw exceptions or behave in other undesirable ways upon receipt of overlapping fragments, which is how the Teardrop attack works to create a DoS. |
| 2000 | 400010 | ICMP Echo Reply | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 0 (Echo Reply). |
| 2001 | 400011 | ICMP Host Unreachable | Informational | Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 3 (Host Unreachable). |
| 2002 | 400012 | ICMP Source Quench | Informational | Triggers when an IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 4 (Source Quench). |

| Signature ID | Message Number | Signature Title | Signature Type | Description |
|---|---|---|---|---|
| 2003 | 400013 | ICMP Redirect | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 5 (Redirect). |
| 2004 | 400014 | ICMP Echo Request | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 8 (Echo Request). |
| 2005 | 400015 | ICMP Time Exceeded for a Datagram | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 11(Time Exceeded for a Datagram). |
| 2006 | 400016 | ICMP Parameter Problem on Datagram | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 12 (Parameter Problem on Datagram). |
| 2007 | 400017 | ICMP Timestamp Request | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 13 (Timestamp Request). |
| 2008 | 400018 | ICMP Timestamp Reply | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 14 (Timestamp Reply). |
| 2009 | 400019 | ICMP Information Request | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 15 (Information Request). |
| 2010 | 400020 | ICMP Information Reply | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 16 (ICMP Information Reply). |
| 2011 | 400021 | ICMP Address Mask Request | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 17 (Address Mask Request). |
| 2012 | 400022 | ICMP Address Mask Reply | Informational | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and the type field in the ICMP header set to 18 (Address Mask Reply). |
| 2150 | 400023 | Fragmented ICMP Traffic | Attack | Triggers when a IP datagram is received with the protocol field of the IP header set to 1 (ICMP) and either the more fragments flag is set to 1 (ICMP) or there is an offset indicated in the offset field. |
| 2151 | 400024 | Large ICMP Traffic | Attack | Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP) and the IP length > 1024. |

| Signature ID | Message Number | Signature Title | Signature Type | Description |
|---|---|---|---|---|
| 2154 | 400025 | Ping of Death Attack | Attack | Triggers when a IP datagram is received with the protocol field of the IP header set to 1(ICMP), the Last Fragment bit is set, and ( IP offset * 8 ) + ( IP data length) > 65535 that is to say, the IP offset (which represents the starting position of this fragment in the original packet, and which is in 8 byte units) plus the rest of the packet is greater than the maximum size for an IP packet. |
| 3040 | 400026 | TCP NULL flags | Attack | Triggers when a single TCP packet with none of the SYN, FIN, ACK, or RST flags set has been sent to a specific host. |
| 3041 | 400027 | TCP SYN+FIN flags | Attack | Triggers when a single TCP packet with the SYN and FIN flags are set and is sent to a specific host. |
| 3042 | 400028 | TCP FIN only flags | Attack | Triggers when a single orphaned TCP FIN packet is sent to a privileged port (having port number less than 1024) on a specific host. |
| 3153 | 400029 | FTP Improper Address Specified | Informational | Triggers if a port command is issued with an address that is not the same as the requesting host. |
| 3154 | 400030 | FTP Improper Port Specified | Informational | Triggers if a port command is issued with a data port specified that is <1024 or >65535. |
| 4050 | 400031 | UDP Bomb attack | Attack | Triggers when the UDP length specified is less than the IP length specified. This malformed packet type is associated with a denial of service attempt. |
| 4051 | 400032 | UDP Snork attack | Attack | Triggers when a UDP packet with a source port of either 135, 7, or 19 and a destination port of 135 is detected. |
| 4052 | 400033 | UDP Chargen DoS attack | Attack | This signature triggers when a UDP packet is detected with a source port of 7 and a destination port of 19. |
| 6050 | 400034 | DNS HINFO Request | Informational | Triggers on an attempt to access HINFO records from a DNS server. |
| 6051 | 400035 | DNS Zone Transfer | Informational | Triggers on normal DNS zone transfers, in which the source port is 53. |
| 6052 | 400036 | DNS Zone Transfer from High Port | Informational | Triggers on an illegitimate DNS zone transfer, in which the source port is not equal to 53. |
| 6053 | 400037 | DNS Request for All Records | Informational | Triggers on a DNS request for all records. |
| 6100 | 400038 | RPC Port Registration | Informational | Triggers when attempts are made to register new RPC services on a target host. |
| 6101 | 400039 | RPC Port Unregistration | Informational | Triggers when attempts are made to unregister existing RPC services on a target host. |

| Signature ID | Message Number | Signature Title | Signature Type | Description |
|---|---|---|---|---|
| 6102 | 400040 | RPC Dump | Informational | Triggers when an RPC dump request is issued to a target host. |
| 6103 | 400041 | Proxied RPC Request | Attack | Triggers when a proxied RPC request is sent to the portmapper of a target host. |
| 6150 | 400042 | ypserv (YP server daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port. |
| 6151 | 400043 | ypbind (YP bind daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port. |
| 6152 | 400044 | yppasswdd (YP password daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port. |
| 6153 | 400045 | ypupdated (YP update daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port. |
| 6154 | 400046 | ypxfrd (YP transfer daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port. |
| 6155 | 400047 | mountd (mount daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the mount daemon (mountd) port. |
| 6175 | 400048 | rexd (remote execution daemon) Portmap Request | Informational | Triggers when a request is made to the portmapper for the remote execution daemon (rexd) port. |
| 6180 | 400049 | rexd (remote execution daemon) Attempt | Informational | Triggers when a call to the rexd program is made. The remote execution daemon is the server responsible for remote program execution. This may be indicative of an attempt to gain unauthorized access to system resources. |
| 6190 | 400050 | statd Buffer Overflow | Attack | Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources. |

## Examples

The following example disables signature 6100:

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

## Related Commands

| Command | Description |
|---|---|
| **ip audit attack** | Sets the default actions for packets that match an attack signature. |
| **ip audit info** | Sets the default actions for packets that match an informational signature. |
| **ip audit interface** | Assigns an audit policy to an interface. |

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

# ip-client

To allow FXOS to initiate management traffic and send it out of a Firepower 2100 ASA data interface, use the **ip-client** command in global configuration mode. To disable traffic initiation, use the **no** form of this command.

**ip-client***interface_name*
**no ip-client** *interface_name*

## Syntax Description

| | |
|---|---|
| *interface_name* | Specifies the interface name through which FXOS can send management traffic. |

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 9.8(2) | We added this command. |

## Usage Guidelines

You can enable FXOS management traffic initiation on ASA data interfaces, which is required for SNMP traps, or NTP and DNS server access, for example. For incoming management traffic, see the **fxos permit** command.

In the FXOS configuration, make sure the default gateway is set to 0.0.0.0, which sets the ASA as the gateway. See the FXOS **set out-of-band** command.

## Examples

The following allows FXOS traffic initiation through the outside interface:

```
ciscoasa(config)# ip-client outside
```

## Related Commands

| Command | Description |
|---|---|
| **connect fxos** | From the ASA CLI, connects to the FXOS CLI. |
| **fxos permit** | Allows FXOS management access on ASA data interfaces. |
| **fxos port** | Sets the FXOS management access port. |

# ip-comp

To enable LZS IP compression, use the **ip-comp enable** command in group-policy configuration mode. To disable IP compression, use the **ip-comp disable** command.To remove the **ip-comp** attribute from the running configuration, use the **no** form of this command.

**ip-comp** { **enable** | **disable** }
**no ip-comp**

## Syntax Description

| | |
|---|---|
| **disable** | Disables IP compression. |
| **enable** | Enables IP compression. |

## Command Default

IP compression is disabled.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Group-policy configuratio | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

The **no** form of this command enables inheritance of a value from another group policy. 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 ASA. 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.

If the endpoints generate IP compression traffic, you should disable IP compression to prevent improper decompression of the packets. If IP compression is enabled on a particular LAN to LAN tunnel, host A cannot communicate with host B when trying to pass IP compression data from one side of the tunnel to other side.

**Note** When the **ip-comp** command is enabled and IPsec fragmentation is configured for "before-encryption," you cannot have IPsec compression (ip-comp_option and pre-encryption). The IP header sent to the crypto chip becomes obfuscated (because of the compression), causing the crypto chip to generate an error when processing the supplied outbound packet. You might also check your MTU level to ensure that it is a small amount (such as 600 bytes).

## Examples

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

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

# ip local pool

To configure IP address pools, use the **ip local pool** command in global configuration mode. To delete the address pool, 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. You cannot use a 255.255.255.254 (/31) or 255.255.255.255 (/32) subnet mask. |
| *poolname* | Specifies the name of the IP address pool. |

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |
| 9.0(1) | IP local pool for the cluster pool in the **ip address** command to support ASA clustering was added. |

## Usage Guidelines

You must supply the mask value when the IP addresses assigned to VPN clients belonging 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.

```
ciscoasa(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 unnumbered

To borrow or inherit an IP address from an interface (for example, a loopback interface), use the **ip unnumbered** command in the interface configuration mode. To stop inheriting an ip address from an interface, use the **no** form of this command.

**ip unnumbered** *interface-name*
**no ip unnumbered**

## Syntax Description

| | |
|---|---|
| *interface-name* | Specifies the name of an interface to inherit the IP address.. |

## Command Default

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 |
| Interface Configuration | • Yes | • Yes | • Yes | • Yes | — |

## Command History

| Release | Modification |
|---|---|
| 9.19(1) | This command was added. |

## Usage Guidelines

The **ip unnumbered** command is used to inherit the IP address of the selected interface as the address for the current interface.

## Examples

The following example borrows the IP address from the loopback interface:

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ip unnumbered loopback1
```

## Related Commands

| Command | Description |
|---|---|
| **ipv6 unnumbered** *interface-name* | Inherits the IPv6 address of the specified interface. |
| **interface loopback** *loopback-number* | Creates a loopback interface. |

# ip-phone-bypass

To enable IP Phone Bypass, use the **ip-phone-bypass enable** command in group-policy configuration mode.To remove the IP phone Bypass attribute from the running configuration, use the **no** form of this command.

**ip-phone-bypass** { **enable** | **disable** }
**no ip-phone-bypass**

## Syntax Description

| | |
|---|---|
| **disable** | Disables IP Phone Bypass. |
| **enable** | Enables IP Phone Bypass. |

## Command Default

IP Phone Bypass is disabled.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

To disable IP Phone Bypass, use the **ip-phone-bypass disable** command. The **no** form of this command option allows inheritance of a value for IP Phone Bypass from another group policy.

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

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

You also need to configure the **mac-exempt** option to exempt the clients from authentication. See the **vpnclient mac-exempt** command for more information.

## Examples

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

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

**Related Commands**

| Command | Description |
|---|---|
| **user-authentication** | Requires users behind a hardware client to identify themselves to the ASA before connecting. |

# ips

To divert traffic from the ASA to the AIP SSM for inspection, use the **ips** command in class configuration mode. To remove this command, use the **no** form of this command.

**ips** { **inline** | **promiscuous** } { **fail-close** | **fail-open** } [ **sensor** { *sensor_name* | *mapped_name* } ]
**no ips** { **inline** | **promiscuous** } { **fail-close** | **fail-open** } [ **sensor** { *sensor_name* | *mapped_name* } ]

## Syntax Description

| | |
|---|---|
| **fail-close** | Blocks traffic if the AIP SSM fails. |
| **fail-open** | Permits traffic if the AIP SSM fails. |
| **inline** | Directs packets to the AIP SSM; the packet might be dropped as a result of IPS operation. |
| **promiscuous** | Duplicates packets for the AIP SSM; the original packet cannot be dropped by the AIP SSM. |
| **sensor** {*sensor_name* \| *mapped_name* } | Sets the virtual sensor name for this traffic. If you use virtual sensors on the AIP SSM (using Version 6.0 or above), you can specify a sensor name using this argument. To see available sensor names, enter the **ips ... sensor ?** command. Available sensors are listed. You can also use the **show ips** command.<br><br>If you use multiple context mode on the ASA, you can only specify sensors that you assigned to the context (see the **allocate-ips** command). Use the *mapped_name* argument if configured in the context.<br><br>If you do not specify a sensor name, then the traffic uses the default sensor. In multiple context mode, you can specify a default sensor for the context. In single mode or if you do not specify a default sensor in multiple mode, the traffic uses the default sensor that is set on the AIP SSM.<br><br>If you enter a name that does not yet exist on the AIP SSM, you get an error, and the command is rejected. |

## Command Default

No default behavior or values.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |
| 8.0(2) | Virtual sensor support was added. |

## Usage Guidelines

The ASA 5500 series supports the AIP SSM, which runs advanced IPS software that provides proactive, full-featured intrusion prevention services to stop malicious traffic, including worms and network viruses, before they can affect your network. Before or after you configure the **ips** command on the ASA, configure the security policy on the AIP SSM. You can either session to the AIP SSM from the ASA (the **session** command) or you can connect directly to the AIP SSM using SSH or Telnet on its management interface. Alternatively, you can use ASDM. For more information about configuring the AIP SSM, see Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface.

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

The AIP SSM runs a separate application from the ASA. It is, however, integrated into the ASA traffic flow. The AIP SSM does not contain any external interfaces itself, other than a management interface. When you apply the **ips** command for a class of traffic on the ASA, traffic flows through the ASA and the AIP SSM in the following way:

1. Traffic enters the ASA.
2. Firewall policies are applied.
3. Traffic is sent to the AIP SSM over the backplane (using the **inline** keyword; See the **promiscuous** keyword for information about only sending a copy of the traffic to the AIP SSM).
4. The AIP SSM applies its security policy to the traffic, and takes appropriate actions.
5. Valid traffic is sent back to the ASA over the backplane; the AIP SSM might block some traffic according to its security policy, and that traffic is not passed on.
6. VPN policies are applied (if configured).
7. Traffic exits the ASA.

## Examples

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic if the AIP SSM card fails for any reason:

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

The following example diverts all IP traffic destined for the 10.1.1.0 network and the 10.2.1.0 network to the AIP SSM in inline mode, and allows all traffic through if the AIP SSM card fails for any reason. For the my-ips-class traffic, sensor1 is used; for the my-ips-class2 traffic, sensor2 is used.

```
ciscoasa(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
```

```
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor2
ciscoasa(config-pmap-c)# service-policy my-ips-policy interface outside
```

## Related Commands

| Command | Description |
|---|---|
| **allocate-ips** | Assigns a virtual sensor to a security context. |
| **class** | Specifies a class map to use for traffic classification. |
| **class-map** | Identifies traffic for use in a policy map. |
| **policy-map** | Configures a policy; that is, an association of a traffic class and one or more actions. |
| **show running-config policy-map** | Displays all current policy map configurations. |

# ipsec-udp

To enable IPsec over UDP, use the **ipsec-udp enable** command in group-policy configuration mode. To remove the IPsec over UDP attribute from the current group policy, use the **no** form of this command.

**ipsec-udp** { **enable** | **disable** }
**no ipsec-udp**

## Syntax Description

| | |
|---|---|
| **disable** | Disables IPsec over UDP. |
| **enable** | Enables IPsec over UDP. |

## Command Default

IPsec over UDP is disabled.

## Command Modes

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

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

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

The **no** form of this command enables inheritance of a value for IPsec over UDP from another group policy.

IPsec over UDP, sometimes called IPsec through NAT, lets a Cisco VPN Client or hardware client connect via UDP to an ASA that is running NAT.

To disable IPsec over UDP, use the **ipsec-udp disable** command.

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, applies only to remote access connections, and requires mode configuration, which means that the ASA exchanges configuration parameters with the client while negotiating SAs.

Using IPsec over UDP may slightly degrade system performance.

The ipsec-udp-port command is not supported on an ASA5505 operating as a VPN client. The ASA 5505 in client mode can initiate IPsec sessions on UDP ports 500 and/or 4500.

## Examples

The following example shows how to configure IPsec over UDP for the group policy named FirstGroup:

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

## Related Commands

| Command | Description |
|---|---|
| **ipsec-udp-port** | Specifies the port on which the ASA 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.

**ipsec-udp-port***port*
**noipsec-udp-port**

## Syntax Description

| | |
|---|---|
| *port* | Identifies the UDP port number using an integer in the range of 4001 through 49151. |

## Command Default

The default port is 10000.

## Command Modes

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

| Command Mode | Firewall Mode | | Security Context | | |
|---|---|---|---|---|---|
| | Routed | Transparent | Single | Multiple | |
| | | | | Context | System |
| Group-policy configuratio | • Yes | — | • Yes | — | — |

## Command History

| Release | Modification |
|---|---|
| 7.0(1) | This command was added. |

## Usage Guidelines

The **no** form of this command enables inheritance of a value for the IPsec over UDP port from another group policy.

In IPsec negotiations. the ASA 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:

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(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 an ASA that is running NAT. |