

Configuring IP Security Options

Cisco provides IP Security Option (IPSO) support as described in RFC 1108. Cisco's implementation is only minimally compliant with RFC 1108 because the Cisco IOS software only accepts and generates a 4-byte IPSO.

IPSO is generally used to comply with the U.S. Government's Department of Defense security policy.

For a complete description of IPSO commands, refer to the "IP Security Options Commands" chapter of the *Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

In This Chapter

This chapter describes how to configure IPSO for both the basic and extended security options described in RFC 1108. This chapter also describes how to configure auditing for IPSO. This chapter includes the following sections:

- Configure Basic IP Security Options
- Configure Extended IP Security Options
- Configure the DNSIX Audit Trail Facility
- IPSO Configuration Examples

Configure Basic IP Security Options

Cisco's basic IPSO support provides the following features:

- Defines security level on a per-interface basis
- Defines single-level or multilevel interfaces
- Provides a label for incoming packets
- Strips labels on a per-interface basis
- Reorders options to put any basic security options first

To configure basic IPSO, complete the tasks in the following sections:

- Enable IPSO and Set the Security Classifications
- Specify How IP Security Options Are Processed

Enable IPSO and Set the Security Classifications

To enable IPSO and set security classifications on an interface, perform either of the following tasks in interface configuration mode:

Task	Command
Set an interface to the requested IPSO classification and authorities.	ip security dedicated <i>level authority [authority...]</i>
Set an interface to the requested IPSO range of classifications and authorities.	ip security multilevel <i>level1 [authority1...] to level2 authority2 [authority2...]</i>

Use the **no ip security** command to reset an interface to its default state.

Specify How IP Security Options Are Processed

To specify how IP security options are processed, perform any of the following optional tasks in interface configuration mode:

Task	Command
Enable an interface to ignore the authorities field of all incoming packets.	ip security ignore-authorities
Classify packets that have no IPSO with an implicit security label.	ip security implicit-labelling [<i>level authority [authority...]</i>]
Accept packets on an interface that has an extended security option present.	ip security extended-allowed
Ensure that all packets leaving the router on an interface contain a basic security option.	ip security add
Remove any basic security option that might be present on a packet leaving the router through an interface.	ip security strip
Prioritize security options on a packet.	ip security first
Treat as valid any packets that have Reserved1 through Reserved4 security levels.	ip security reserved-allowed

Default Values for Command Keywords

In order to fully comply with IPSO, the default values for the minor keywords have become complex. Default value usages include the following:

- The default for all of the minor keywords is *off*, with the exception of **implicit-labelling** and **add**.
- The default value of **implicit-labelling** is *on* if the interface is unclassified Genser; otherwise, it is *off*.
- The default value for **add** is *on* if the interface is not “unclassified Genser”; otherwise, it is *off*.

Table 18 provides a list of all default values.

Table 18 Default Security Keyword Values

Interface Type	Level	Authority	Implicit Labeling	Add IPSO
None	None	None	On	Off
Dedicated	Unclassified	Genser	On	Off
Dedicated	Any	Any	Off	On
Multilevel	Any	Any	Off	On

The default value for any interface is “dedicated, unclassified Genser.” Note that this implies implicit labeling. This might seem unusual, but it makes the system entirely transparent to packets without options. This is the setting generated when you specify the **no ip security** interface configuration command.

Configure Extended IP Security Options

Our extended IPSO support is compliant with the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) specification documents. Extended IPSO functionality can unconditionally accept or reject Internet traffic that contains extended security options by comparing those options to configured allowable values. This support allows DNSIX networks to use additional security information to achieve a higher level of security than that achievable with basic IPSO.

We also support a subset of the security features defined in the DNSIX Version 2.1 specification. Specifically, we support DNSIX definitions of the following:

- How extended IPSO is processed
- Audit trail facility

There are two kinds of extended IPSO fields defined by the DNSIX 2.1 specification and supported by our implementation of extended IPSO—Network Level Extended Security Option (NLESO) and Auxiliary Extended Security Option (AESO) fields.

NLESO processing requires that security options be checked against configured allowable information, source, and compartment bit values, and requires that the router be capable of inserting extended security options in the IP header.

AESO is similar to NLESO, except that its contents are not checked and are assumed to be valid if its source is listed in the AESO table.

To configure extended IPSO, complete the tasks in the following sections:

- Configure Global Default Settings
- Attach ESOs to an Interface
- Attach AESOs to an Interface

DNSIX Version 2.1 causes slow-switching code.

See the “IPSO Configuration Examples” section at the end of this chapter.

Configure Global Default Settings

To configure global default setting for extended IPSO, including AESOs, perform the following task in global configuration mode:

Task	Command
Configure system-wide default settings.	ip security eso-info <i>source compartment-size default-bit</i>

Attach ESOs to an Interface

To specify the minimum and maximum sensitivity levels for an interface, perform the following tasks in interface configuration mode:

Task	Command
Set the minimum sensitivity level for an interface.	ip security eso-min <i>source compartment-bits</i>
Set the maximum sensitivity level for an interface.	ip security eso-max <i>source compartment-bits</i>

Attach AESOs to an Interface

To specify the extended IPSO sources that are to be treated as AESO sources, perform the following task in interface configuration mode:

Task	Command
Specify AESO sources.	ip security aeso <i>source compartment-bits</i>

Configure the DNSIX Audit Trail Facility

The audit trail facility is a UDP-based protocol that generates an audit trail of IPSO security violations. This facility allows the system to report security failures on incoming and outgoing packets. The Audit Trail Facility sends DNSIX audit trail messages when a datagram is rejected because of IPSO security violations. This feature allows you to configure organization-specific security information.

The DNSIX audit trail facility consists of two protocols:

- DNSIX Message Deliver Protocol (DMDP) provides a basic message-delivery mechanism for all DNSIX elements.
- Network Audit Trail Protocol (NAT) provides a buffered logging facility for applications to use to generate auditing information. This information is then passed on to DMDP.

To configure the DNSIX auditing facility, complete the tasks in the following sections:

- Enable the DNSIX Audit Trail Facility
- Specify Hosts to Receive Audit Trail Messages
- Specify Transmission Parameters

Enable the DNSIX Audit Trail Facility

To enable the DNSIX audit trail facility, perform the following task in global configuration mode:

Task	Command
Start the audit writing module.	dnsix-nat source <i>ip-address</i>

Specify Hosts to Receive Audit Trail Messages

To define and change primary and secondary addresses of the host to receive audit messages, perform the following tasks in global configuration mode:

Task	Command
Specify the primary address for the audit trail	dnsix-nat primary <i>ip-address</i>
Specify the secondary address for the audit trail.	dnsix-nat secondary <i>ip-address</i>
Specify the address of a collection center that is authorized to change primary and secondary addresses. Specified hosts are authorized to change the destination of audit messages.	dnsix-nat authorized-redirection <i>ip-address</i>

Specify Transmission Parameters

To specify transmission parameters, perform the following tasks in global configuration mode:

Task	Command
Specify the number of records in a packet before it is sent to a collection center.	dnsix-nat transmit-count <i>count</i>
Specify the number of transmit retries for DMDP.	dnsix-dmdp retries <i>count</i>

IPSO Configuration Examples

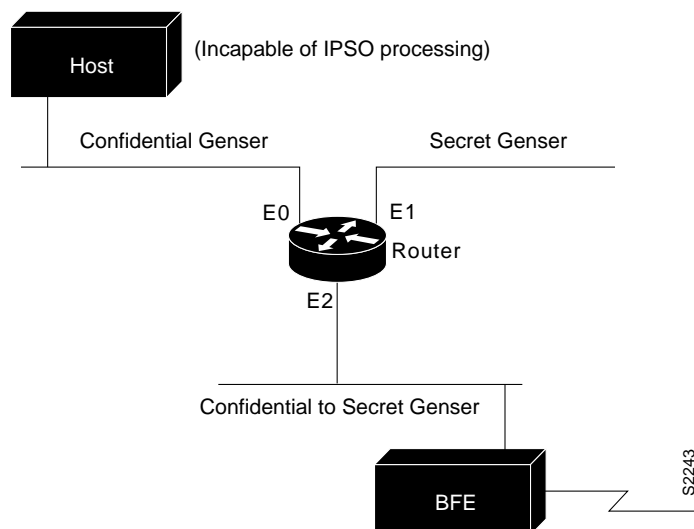
There are two examples in this section:

- Example 1
- Example 2
- Example 3

Example 1

In this example, three Ethernet interfaces are presented. These interfaces are running at security levels of Confidential Genser, Secret Genser, and Confidential to Secret Genser, as shown in Figure 18.

Figure 18 IPSO Security Levels



The following commands set up interfaces for the configuration in Figure 18:

```
interface ethernet 0
 ip security dedicated confidential genser
interface ethernet 1
 ip security dedicated secret genser
interface ethernet 2
 ip security multilevel confidential genser to secret genser
```

It is possible for the setup to be much more complex.

Example 2

In the following example, there are devices on Ethernet 0 that cannot generate a security option, and so must accept packets without a security option. These hosts do not understand security options; therefore, never place one on such interfaces. Furthermore, there are hosts on the other two networks that are using the extended security option to communicate information, so you must allow these to pass through the system. Finally, there also is a host (a Blacker Front End; see the “Configuring X.25 and LABP” chapter of the *Wide-Area Networking Configuration Guide* for more information about Blacker emergency mode) on Ethernet 2 that requires the security option to be the first option present, and this condition also must be specified. The new configuration follows.

```
interface ethernet 0
  ip security dedicated confidential genser
  ip security implicit-labelling
  ip security strip
interface ethernet 1
  ip security dedicated secret genser
  ip security extended-allowed
!
interface ethernet 2
  ip security multilevel confidential genser to secret genser
  ip security extended-allowed
  ip security first
```

Example 3

This example configures a Cisco router with HP-UX CMW DNSIX hosts. The following commands should be configured on each LAN interface of the router in order for two DNSIX hosts to communicate:

```
ip security multilevel unclassified nsa to top secret nsa
ip security extended allowed
```

DNSIX hosts do not need to know the router’s IP addresses, and DNSIX hosts do not need to set up M6RHDB entries for the routers.

