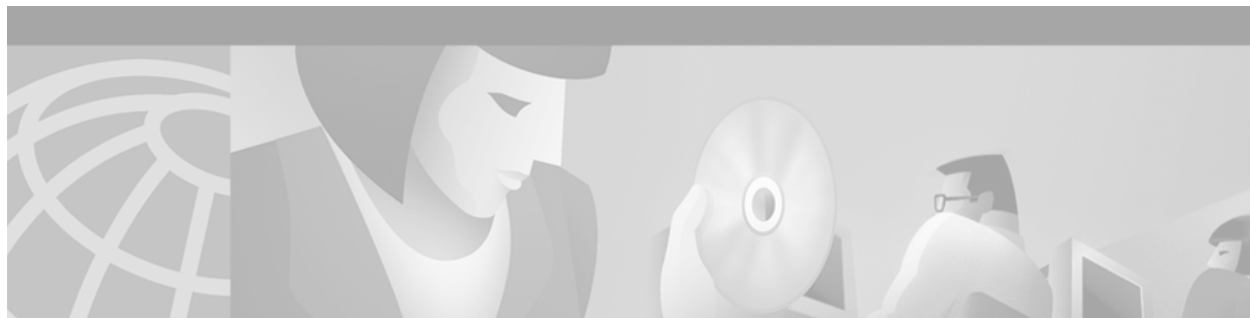




Cisco IOS Firewall Intrusion Detection System Commands

This chapter describes the commands used to configure the integrated Intrusion Detection System (IDS) features in Cisco IOS Firewall. Intrusion detection systems provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. The IDS technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

The Cisco IOS Firewall IDS feature identifies 59 of the most common attacks using “signatures” to detect patterns of misuse in network traffic. For a description of Cisco IOS Firewall IDS signatures, refer to the “Integrated Intrusion Detection System” section in the *Cisco IOS Security Configuration Guide*.

Using Cisco IOS Firewall IDS, the Cisco IOS Firewall acts as an in-line intrusion detection sensor, watching packets and sessions as they flow through the router, scanning each to match any of the Cisco IOS Firewall IDS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog. The network administrator can configure Cisco IOS Firewall IDS to choose the appropriate response to various threats. When packets in a session match a signature, Cisco IOS Firewall IDS can be configured to perform the following tasks:

- Send an alarm to a syslog server or a NetRanger Director (centralized management interface)
- Drop the packet
- Reset the TCP connection

The IDS feature in Cisco IOS Firewall is compatible with Cisco Secure Intrusion Detection System (formally known as NetRanger). The Cisco Secure IDS is an enterprise-scale, real-time, intrusion detection system designed to detect, report, and terminate unauthorized activity throughout a network.

The Cisco Secure IDS consists of three components: Sensor, Director, and Post Office. Cisco Secure IDS Sensors analyze the content and context of individual packets to determine if traffic is authorized. The Cisco Secure IDS Director is a software-based management system that centrally monitors the activity of multiple Cisco Secure IDS Sensors. The Cisco Secure IDS Post Office is the communication backbone that allows NetRanger services and hosts to communicate with each other.

The IDS feature in Cisco IOS Firewall can be added to the NetRanger Director screen as an icon to provide a consistent view of all intrusion detection sensors throughout a network. It also can be configured to permit logging to the NetRanger Director console in addition to Cisco IOS syslog. For additional information about Cisco Secure IDS (NetRanger), refer to the *NetRanger User Guide*.

For more information on how to configure Cisco IOS Firewall IDS, refer to the “Configuring Integrated Intrusion Detection System” chapter in the *Cisco IOS Security Configuration Guide*. For configuration examples, refer to the Cisco IOS Firewall “IDS Configuration Examples” section in the “Configuring Integrated Intrusion Detection System” chapter of the *Cisco IOS Security Configuration Guide*.

clear ip audit configuration

To disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources, use the **clear ip audit configuration** EXEC command.

clear ip audit configuration

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Use the clear ip audit configuration EXEC command to disable Cisco IOS Firewall IDS, remove all intrusion detection configuration entries, and release dynamic resources.
-------------------------	--

Examples	The following example clears the existing IP audit configuration: <pre>clear ip audit configuration</pre>
-----------------	--

clear ip audit statistics

To reset statistics on packets analyzed and alarms sent, use the **clear ip audit statistics** EXEC command.

clear ip audit statistics

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Use the clear ip audit statistics EXEC command to reset statistics on packets analyzed and alarms sent.
-------------------------	--

Examples	The following example clears all IP audit statistics: <pre>clear ip audit statistics</pre>
-----------------	---

ip audit

To apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction, use the **ip audit** interface configuration command. To disable auditing of the interface for the specified direction, use the **no** version of this command.

```
ip audit audit-name {in | out}

no ip audit audit-name {in | out}
```

Syntax Description	<i>audit-name</i>	Name of an audit specification.
	in	Inbound traffic.
	out	Outbound traffic.

Defaults No audit specifications are applied to an interface or direction.

Command Modes Interface configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **ip audit** interface configuration command to apply an audit specification created with the **ip audit** command to a specific interface and for a specific direction.

Examples In the following example, the audit specification MARCUS is applied to an interface and direction:

```
interface e0
ip audit MARCUS in
```

In the following example, the audit specification MARCUS is removed from the interface on which it was previously added:

```
interface e0
no ip audit MARCUS in
```

ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** global configuration command. To set the default action for attack signatures, use the **no** form of this command.

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

no ip audit attack

Syntax Description	action	Specifies an action for the attack signature to take in response to a match.
	alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.
	drop	(Optional) Drops the packet. Used with the action keyword.
	reset	(Optional) Resets the TCP session. Used with the action keyword.

Defaults	The default action is alarm .
----------	--------------------------------------

Command Modes	Global configuration
---------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Use the ip audit attack global configuration command to specify the default actions for attack signatures.
------------------	---

Examples	In the following example, the default action for attack signatures is set to all three actions: <pre>ip audit attack action alarm drop reset</pre>
----------	---

ip audit info

To specify the default actions for info signatures, use the **ip audit info** global configuration command. To set the default action for info signatures, use the **no** form of this command.

```
ip audit info { action [alarm] [drop] [reset] }  
  
no ip audit info
```

Syntax Description

action	Sets an action for the info signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.
drop	(Optional) Drops the packet. Used with the action keyword.
reset	(Optional) Resets the TCP session. Used with the action keyword.

Defaults

The default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Use the **ip audit info** global configuration command. to specify the default actions for info signatures.

Examples

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```

ip audit name

To create audit rules for info and attack signature types, use the **ip audit name** global configuration command. To delete an audit rule, use the **no** form of this command.

ip audit name *audit-name* { **info** | **attack** } [**list** *standard-acl*] [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *audit-name* { **info** | **attack** }

Syntax Description

<i>audit-name</i>	Name for an audit specification.
info	Specifies that the audit rule is for info signatures.
attack	Specifies that the audit rule is for attack signatures.
list	(Optional) Specifies an ACL to attach to the audit rule.
<i>standard-acl</i>	(Optional) Integer representing an access control list. Use with the list keyword.
action	(Optional) Specifies an action or actions to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the action keyword.
drop	(Optional) Drops the packet. Use with the action keyword.
reset	(Optional) Resets the TCP session. Use with the action keyword.

Defaults

If an action is not specified, the default action is **alarm**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Any signatures disabled with the **ip audit signature** command do not become a part of the audit rule created with the **ip audit name** command.

Examples

In the following example, an audit rule called INFO.2 is created, and configured with all three actions:

```
ip audit name INFO.2 info action alarm drop reset
```

In the following example, an info signature is disabled and an audit rule called INFO.3 is created:

```
ip audit signature 1000 disable
ip audit name INFO.3 info action alarm drop reset
```

In the following example, an audit rule called ATTACK.2 is created with an attached ACL 91, and the ACL is created:

```
ip audit name ATTACK.2 list 91
access-list 91 deny 10.1.0.0 0.0.255.255
access-list 91 permit any
```

ip audit notify

To specify the method of event notification, use the **ip audit notify** global configuration command. To disable event notifications, use the **no** form of this command.

ip audit notify {nr-director | log}

no ip audit notify {nr-director | log}

Syntax Description

nr-director	Send messages in NetRanger format to the NetRanger Director or Sensor.
log	Send messages in syslog format.

Defaults

The default is to send messages in syslog format.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

If messages are sent to the NetRanger Director, then you must also configure the NetRanger Director's Post Office transport parameters using the **ip audit po remote** command.

Examples

In the following example, event notifications are specified to be sent in NetRanger format:

```
ip audit notify nr-director
```

Related Commands

Command	Description
ip audit po local	Specifies the local Post Office parameters used when sending event notifications to the NetRanger Director.
ip audit po remote	Specifies one or more sets of Post Office parameters for NetRanger Directors receiving event notifications from the router.

ip audit po local

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the **ip audit po local** global configuration command. To set the local Post Office parameters to their default settings, use the **no** form of this command.

ip audit po local **hostid** *id-number* **orgid** *id-number*

no ip audit po local [**hostid** *id-number* **orgid** *id-number*]

Syntax Description	hostid	Specifies a NetRanger host ID.
	<i>id-number</i> (hostid)	Unique integer in the range 1-65535 used in NetRanger communications to identify the local host. Use with the hostid keyword.
	orgid	Specifies a NetRanger organization ID.
	<i>id-number</i> (orgid)	Unique integer in the range 1-65535 used in NetRanger communications to identify the group to which the local host belongs. Use with the orgid keyword.

Defaults The default organization ID is 1. The default host ID is 1.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **ip audit po local** global configuration command to specify the local Post Office parameters used when sending event notifications to the NetRanger Director.

Examples In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip audit po local hostid 10 orgid 500
```

ip audit po max-events

To specify the maximum number of event notifications that are placed in the router's event queue, use the **ip audit po max-events** global configuration command. To set the number of recipients to the default setting, use the **no** version of this command.

ip audit po max-events *number-of-events*

no ip audit po max-events

Syntax Description

number-of-events

Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events.

Defaults

The default number of events is 100.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Examples

In the following example, the number of events in the event queue is set to 250:

```
ip audit po max-events 250
```

ip audit po protected

To specify whether an address is on a protected network, use the **ip audit po protected** global configuration command. To remove network addresses from the protected network list, use the **no** form of this command. If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

ip audit po protected *ip-addr* [**to** *ip-addr*]

no ip audit po protected [*ip-addr*]

Syntax Description	to	(Optional) Specifies a range of IP addresses.
	<i>ip-addr</i>	IP address of a network host.

Defaults	If no addresses are defined as protected, then all addresses are considered outside the protected network.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	You can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source and/or destination of the packet belongs to a protected network or not.
-------------------------	---

Examples	In the following example, a range of addresses is added to the protected network list:
-----------------	--

```
ip audit po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip audit po protected 10.4.1.1
ip audit po protected 10.4.1.8
ip audit po protected 10.4.1.25
```

In the following example, an address is removed from the protected network list:

```
no ip audit po protected 10.4.1.1
```

ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** global configuration command. To remove a NetRanger Director's Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

```
ip audit po remote hostid host-id orgid org-id rmtaddress ip-address localaddress ip-address
[port port-number] [preference preference-number] [timeout seconds] [application { director
| logger }]
```

```
no ip audit po remote hostid host-id orgid org-id rmtaddress ip-address
```

Syntax Description

<i>host-id</i>	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. Use with the hostid keyword.
hostid	Specifies a NetRanger host ID.
<i>org-id</i>	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the orgid keyword.
orgid	Specifies a NetRanger organization ID.
rmtaddress	Specifies the IP address of the NetRanger Director.
localaddress	Specifies the IP address of the Cisco IOS Firewall IDS router.
<i>ip-address</i>	IP address of the NetRanger Director or Cisco IOS Firewall IDS router's interface. Use with the rmtaddress and localaddress keywords.
<i>port-number</i>	(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. Use with the port keyword.
port	(Optional) Specifies a User Datagram Protocol port through which to send messages.
preference	(Optional) Specifies a route preference for communication.
<i>preference-number</i>	(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the preference keyword.
<i>seconds</i>	(Optional) Integer representing the heartbeat timeout value for Post Office communications. Use with the timeout keyword.
timeout	(Optional) Specifies a timeout value for Post Office communications.
application	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages.
director	(Optional) Specifies that the receiving application is the NetRanger Director interface.
logger	(Optional) Specifies that the receiving application is a NetRanger Sensor.

Defaults

The default organization ID is 1.

The default host ID is 1.

The default UDP port number is 45000.

The default preference is 1.

The default heartbeat timeout is 5 seconds.

The default application is **director**.

Command Modes Global configuration

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines A router can report to more than one NetRanger Director. In this case, use the **ip audit po remote** command to add each NetRanger Director to which the router sends notifications.

More than one route can be established to the same NetRanger Director. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

A router can also report to a NetRanger Sensor. In this case, use the **ip audit po remote** command and specify **logger** as the application.

Examples In the following example, two communication routes for the same dual-homed NetRanger Director are defined:

```
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1
preference 1
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1
preference 2
```

The router uses the first entry to establish communication with the NetRanger Director defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different Director is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip audit po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout
10 application director
```

ip audit signature

To attach a policy to a signature, use the **ip audit signature** global configuration command. You can set two policies: disable a signature or qualify the audit of a signature with an access list. To remove the policy, use the **no** form of this command. If the policy disabled a signature, then the **no** form of this command reenables the signature. If the policy attached an access list to the signature, the **no** form of this command removes the access list.

ip audit signature *signature-id* { **disable** | **list** *acl-list* }

no ip audit signature *signature-id*

Syntax Description

<i>signature-id</i>	Unique integer specifying a signature as defined in the NetRanger Network Security Database.
disable	Disables the ACL associated with the signature.
list	Specifies an ACL to associate with the signature.
<i>acl-list</i>	Unique integer specifying a configured ACL on the router. Use with the list keyword.

Defaults

No policy is attached to a signature.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.

Usage Guidelines

This command is mostly used to disable the auditing of a signature or to exclude some hosts or network segments from being audited.

If you are attaching an access control list to a signature, then you also need to create an audit rule with the **ip audit name** command and apply it to an interface with the **ip audit** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip audit signature 6150 disable
ip audit signature 1000 list 99

access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip audit smtp

To specify the number of recipients in a mail message over which a spam attack is suspected, use the **ip audit smtp** global configuration command. To set the number of recipients to the default setting, use the **no** form of this command.

ip audit smtp spam *number-of-recipients*

no ip audit smtp spam

Syntax Description	spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
	<i>number-of-recipients</i>	Integer in the range of 1–65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the spam keyword. The default is 250 recipients.

Defaults	The default number of recipients is 250.
-----------------	--

Command Modes	Global configuration
----------------------	----------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Use the ip audit smtp global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.
-------------------------	--

Examples	In the following example, the number of recipients is set to 300: <pre>ip audit smtp spam 300</pre>
-----------------	--

show ip audit configuration

To display additional configuration information, including default values that may not be displayed using the **show run** command, use the **show ip audit configuration EXEC** command.

show ip audit configuration

Syntax Description This command has no argument or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **show ip audit configuration EXEC** command to display additional configuration information, including default values that may not be displayed using the **show run** command.

Examples The following example displays the output of the **show ip audit configuration** command:

```
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
  Audit name AUDIT.1
    info actions alarm
```

Related Commands	Command	Description
	clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip audit interface

To display the interface configuration, use the **show ip audit interface** EXEC command.

show ip audit interface

Syntax Description	This command has no arguments or keywords.
---------------------------	--

Command Modes	EXEC
----------------------	------

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines	Use the show ip audit interface EXEC command to display the interface configuration.
-------------------------	---

Examples	The following example displays the output of the show ip audit interface command:
-----------------	--

```
Interface Configuration
Interface Ethernet0
  Inbound IDS audit rule is AUDIT.1
  info actions alarm
  Outgoing IDS audit rule is not set
Interface Ethernet1
  Inbound IDS audit rule is AUDIT.1
  info actions alarm
  Outgoing IDS audit rule is AUDIT.1
  info actions alarm
```

show ip audit statistics

To display the number of packets audited and the number of alarms sent, among other information, use the **show ip audit statistics** EXEC command.

show ip audit statistics

Syntax Description This command has no arguments or keywords.

Command Modes EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.

Usage Guidelines Use the **show ip audit statistics** EXEC command to display the number of packets audited and the number of alarms sent, among other information.

Examples The following displays the output of the **show ip audit statistics** command:

```
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never
```

```
HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Related Commands	Command	Description
	clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.