



Cisco IOS Firewall Intrusion Detection System

This feature module describes the Cisco IOS Firewall Intrusion Detection feature. It includes information on the benefits of the new feature, supported platforms, related documents, and so forth.

This document includes the following sections:

- Feature Overview on page 2
- Supported Platforms on page 4
- Supported Standards, MIBs, and RFCs on page 4
- Configuration Tasks on page 5
- Configuration Examples on page 10
- Command Reference on page 15
- Message Formats on page 35
- Cisco IOS IDS Signature List on page 36
- Glossary on page 40

Feature Overview

The Cisco IOS Firewall now includes intrusion detection technology for mid-range and high-end router platforms with firewall support. It is ideal for any network perimeter, and especially for locations in which a router is being deployed and additional security between network segments is required. It also can protect intranet and extranet connections where additional security is mandated, and branch-office sites connecting to the corporate office or Internet.

The Cisco IOS Firewall's Intrusion Detection System (Cisco IOS IDS) identifies 59 of the most common attacks using signatures to detect patterns of misuse in network traffic. The intrusion-detection signatures included in the new release of the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures. The signatures represent severe breaches of security and the most common network attacks and information-gathering scans.

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 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 the IDS system to choose the appropriate response to various threats. When packets in a session match a signature, the IDS system can be configured to:

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

Cisco developed its Cisco IOS software-based intrusion-detection capabilities in the Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Also, while it is preferable to enable both the firewall and intrusion detection features of the CBAC security engine to support a network security policy, each of these features may be enabled independently and on different router interfaces. Cisco IOS software-based intrusion detection is part of the Cisco IOS Firewall available on the Cisco 2600, 3600, 7100, and 7200 series routers.

Functional Description

The Cisco IOS IDS acts as an in-line intrusion detection sensor, watching packets as they traverse the router's interfaces and acting upon them in a definable fashion. When a packet, or a number of packets in a session, match a signature, the Cisco IOS IDS may perform the following configurable actions:

- Alarm—Sends an alarm to a syslog server or NetRanger Director
- Drop—Drops the packet
- Reset—Resets the TCP connection

The following describes the packet auditing process with Cisco IOS IDS:

- 1 You create an audit rule, which specifies the signatures that should be applied to packet traffic and the actions to take when a match is found. An audit rule can apply informational and attack signatures to network packets. The signature list can have just one signature, all signatures, or any number of signatures in between. Signatures can be disabled in case of false positives or the needs of the network environment.
- 2 You apply the audit rule to an interface on the router, specifying a traffic direction (*in* or *out*).

- 3 If the audit rule is applied to the *in* direction of the interface, packets passing through the interface are audited before the inbound ACL has a chance to discard them. This allows an administrator to be alerted if an attack or information-gathering activity is underway even if the router would normally reject the activity.
- 4 If the audit rule is applied to the *out* direction on the interface, packets are audited after they enter the router through another interface. In this case, the inbound ACL of the other interface may discard packets before they are audited. This may result in the loss of IDS alarms even though the attack or information-gathering activity was thwarted.
- 5 Packets going through the interface that match the audit rule are audited by a series of modules, starting with IP; then either ICMP, TCP, or UDP (as appropriate); and finally, the Application level.
- 6 If a signature match is found in a module, then the following user-configured action(s) occur:
 - If the action is **alarm**, then the module completes its audit, sends an alarm, and passes the packet to the next module.
 - If the action is **drop**, then the packet is dropped from the module, discarded, and not sent to the next module.
 - If the action is **reset**, then the packets are forwarded to the next module, and packets with the reset flag set are sent to both participants of the session, if the session is TCP.

Note It is recommended that you use the **drop** and **reset** actions together.

If there are multiple signature matches in a module, only the first match fires an action. Additional matches in other modules fire additional alarms, but only one per module.

Note This process is different than on the NetRanger Sensor appliance, which identifies all signature matches for each packet.

Memory and Performance Impact

The performance impact of intrusion detection will depend on the number of signatures enabled, the level of traffic on the router, the router platform, and other individual features enabled on the router such as encryption, source route bridging, and so on. Because this router is being used as a security device, no packet will be allowed to bypass the security mechanisms. The IDS process in the Cisco IOS Firewall router sits directly in the packet path and thus will search each packet for signature matches. In some cases, the entire packet will need to be searched, and state information and even application state and awareness must be maintained by the router.

For auditing atomic signatures, there is no traffic-dependent memory requirement. For auditing compound signatures, CBAC allocates memory to maintain the state of each session for each connection. Memory is also allocated for the configuration database and for internal caching.

Benefits

Intrusion detection systems (IDSes) provide a level of protection beyond the firewall by protecting the network from internal and external attacks and threats. Cisco IOS Firewall IDS technology enhances perimeter firewall protection by taking appropriate action on packets and flows that violate the security policy or represent malicious network activity.

Cisco IOS Firewall intrusion detection capabilities are ideal for providing additional visibility at intranet, extranet, and branch-office Internet perimeters. Network administrators now enjoy more robust protection against attacks on the network and can automatically respond to threats from internal or external hosts.

NetRanger IDS customers can deploy the Cisco IOS software-based IDS signatures to complement their existing IDS systems. This allows an IDS to be deployed to areas that may not be capable of supporting a NetRanger Sensor. Cisco IOS IDS signatures can be deployed alongside or independently of other Cisco IOS Firewall features.

The Cisco IOS Firewall with intrusion detection can be added to the NetRanger Director screen as an icon to provide a consistent view of all intrusion detection sensors throughout a network. The Cisco IOS Firewall intrusion detection capabilities have an enhanced reporting mechanism that permits logging to the NetRanger Director console in addition to Cisco IOS syslog.

The Cisco IOS Firewall with intrusion detection is intended to satisfy the security goals of all of our customers, and is particularly appropriate for:

- Enterprise customers that are interested in a cost-effective method of extending their perimeter security across all network boundaries, specifically branch-office, intranet, and extranet perimeters.
- Small and medium-sized businesses that are looking for a cost-effective router that has an integrated firewall with intrusion-detection capabilities.
- Service provider customers that want to set up managed services, providing firewalling and intrusion detection to their customers, all housed within the necessary function of a router.

Supported Platforms

Cisco IOS intrusion detection capability is integrated with the Cisco IOS Firewall feature set on the following platforms:

- Cisco 2600
- Cisco 3600
- Cisco 7100
- Cisco 7200

Additional platform support is planned for future Cisco IOS software releases.

Supported Standards, MIBs, and RFCs

None

Configuration Tasks

See the following sections for configuration tasks for the Cisco IOS Firewall Intrusion Detection feature. Each task in the list indicates if it is optional or required:

- Initializing Cisco IOS IDS (Required)
- Initializing the Post Office (Required)
- Configuring and Applying Audit Rules (Required)
- Verifying the Configuration (Optional)

Initializing Cisco IOS IDS

The following tasks are necessary for initializing Cisco IOS IDS on a router:

- Step 1** Log on to the router.
- Step 2** Enter enable mode by typing **en** followed by the enable password.
- Step 3** Type **conf t** to enter configuration mode.
- Step 4** Use the **ip audit smtp** command to set the threshold beyond which spamming in e-mail messages is suspected:
- ```
ip audit smtp spam recipients
```
- where *recipients* is the maximum number of recipients in an e-mail message. The default is 250.
- Step 5** Use the **ip audit po max-events** command to set the threshold beyond which queued events are dropped from the queue for sending to the NetRanger Director:
- ```
ip audit po max-events number_events
```
- where *number_events* is the number of events in the event queue. The default is 100. Increasing this number may have an impact on memory and performance, as each event in the event queue requires 32 KB of memory.
- Step 6** Type **exit** to leave terminal configuration mode.

Initializing the Post Office

The following tasks are necessary for initializing the Post Office system:

- Step 1** Enter enable mode by typing **en** followed by the enable password.
- Step 2** Type **conf t** to enter configuration mode.
- Step 3** Use the **ip audit notify** command to send event notifications (alarms) to either a NetRanger Director or syslog server.
- If you are sending alarms to a NetRanger Director, use the following command:
- ```
ip audit notify nr-director
```
- If you are sending alarms to a syslog server, use the following command:
- ```
ip audit notify log
```

Step 4 If you are sending alarms to a NetRanger Director, you must set the Post Office parameters for both the router (using the **ip audit po local** command) and the NetRanger Director (using the **ip audit po remote** command).

(a) First, set the parameters for the router:

```
ip audit po local hostid host-id orgid org-id
```

where *host-id* is a unique number between 1 and 65535 that identifies the router, and *org-id* is a unique number between 1 and 65535 that identifies the organization to which the router and Director both belong.

(b) Next, set the parameters for the NetRanger Director:

```
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 application-type
```

where:

- *host-id* is a unique number between 1 and 65535 that identifies the Director
- *org-id* is a unique number between 1 and 65535 that identifies the organization to which the router and Director both belong
- **rmtaddress** *ip-address* is the Director's IP address
- **localaddress** *ip-address* is the router's interface IP address
- *port-number* identifies the UDP port on which the Director is listening for alarms (45000 is the default)
- *preference-number* is the relative priority of the route to the Director (1 is the default)—if more than one route is used to reach the same Director, then one must be a primary route (preference 1) and the other a secondary route (preference 2)
- *seconds* is the number of seconds the Post Office waits before it determines that a connection has timed out (5 is the default)
- *application-type* is either **director** or **logger**

Note If you are sending Post Office notifications to a Sensor, follow the preceding steps but use **logger** instead of **director** as your application. Sending to a logging application means that no alarms are sent to a GUI; instead, the NetRanger alarm data is written to a flat file, which can then be processed with filters, such as **perl** and **awk**, or staged to a database.

Step 5 If you are sending alarms to the syslog console, you have the option of seeing the syslog messages on the router console.

In terminal configuration mode, turn on logging to the console:

```
logging console info
```

Use the **no logging console info** command to turn off this feature.

- Step 6** Add the IOS IDS router's Post Office information to the `/usr/nr/etc/hosts` and `/usr/nr/etc/routes` files on all NetRanger Sensors and Directors communicating with the router.
- You can do this with the `nrConfigure` tool. For more information, refer to the *NetRanger User Guide*.
- Step 7** Type `exit` to leave terminal configuration mode.
- Step 8** Type `wr mem` to save the configuration.
- Step 9** Reload the router with the `reload` command.

Note You must reload the router every time you make a Post Office configuration change.

Configuring and Applying Audit Rules

The following tasks are necessary for configuring and applying audit rules:

- Step 1** Enter enable mode by typing `en` followed by the enable password.
- Step 2** Type `conf t` to enter configuration mode.
- Step 3** Use the `ip audit info` and `ip audit attack` commands to set the default actions for info and attack signatures. Both types of signatures can take any or all of the following actions: alarm, drop, and reset. For example:

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

- Step 4** Use the `ip audit name` command to create audit rules:

```
ip audit name audit-name info
ip audit name audit-name attack
```

where *audit-name* is a user-defined name for an audit rule.

Note Use the same name when you assign attack and info type signatures.

- Step 5** You can also attach ACLs to an audit rule:

```
ip audit name audit-name {info|attack} list acl-list
```

where *acl-list* is an integer representing an ACL. If you attach an ACL to an audit rule, it must be defined as well.

In the following example, ACL 99 is attached to the audit rule INFO, and ACL 99 is defined:

```
ip audit name INFO info list 99
access-list 99 deny 10.1.1.0 0.0.0.255
access-list 99 permit any
```

Note The ACL in the preceding example is *not* denying traffic from the 10.1.1.0 network (as expected if it were applied to an interface). Instead, the hosts on that network are not filtered through the audit process because they are trusted hosts. On the other hand, all other hosts, as defined by **permit any**, are processed by the audit rule.

Step 6 You can use the **ip audit signature** command to disable individual signatures. Disabled signatures are not included in audit rules, as this is a global configuration change:

```
ip audit signature signature-number disable
```

To re-enable a disabled signature, use the **no ip audit signature** command:

```
no ip audit signature signature-number
```

where *signature-number* is the number of the disabled signature.

Step 7 You can also use the **ip audit signature** command to apply ACLs to individual signatures:

```
ip audit signature signature-number list acl-list
```

where *signature-number* is the number of a signature, and *acl-list* is an integer representing an ACL.

For example, ACL 35 is attached to the 1234 signature, and then defined:

```
ip audit signature 1234 list 35
access-list 35 deny 10.1.1.0 0.0.0.255
access-list 35 permit any
```

Note The ACL in the preceding example is *not* denying traffic from the 10.1.1.0 network (as expected if it were applied to an interface). Instead, the hosts on that network are not filtered through the signature because they are trusted hosts or are otherwise causing false positives to occur. On the other hand, all other hosts, as defined by **permit any**, are processed by the signature.

Step 8 To apply the created audit rule(s), enter interface configuration mode and apply the rule to an interface and direction using the **ip audit** command:

```
int e0
ip audit audit-name direction
```

where *audit-name* is the name of an existing audit rule, and *direction* is either **in** or **out**.

Step 9 Type **exit** to leave interface configuration mode.

Step 10 After you apply the audit rules to the router interfaces, use the **ip audit po protected** command to configure which network should be protected by the router:

```
ip audit po protected ip_addr [to ip_addr]
```

where *ip_addr* is an IP address to protect.

Step 11 Type **exit** to leave terminal configuration mode.

Verifying the Configuration

You can verify that Cisco IOS IDS is properly configured with the **show ip audit configuration** command (see Example 1).

Example 1 Output from show ip audit configuration Command

```
ids2611#show ip audit configuration
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 drop reset
Default threshold of recipients for spam signature is 25
PostOffice:HostID:55 OrgID:123 Msg dropped:0
          :Curr Event Buf Size:100 Configured:100
HID:14 OID:123 S:1 A:2 H:82 HA:49 DA:0 R:0 Q:0
  ID:1 Dest:10.1.1.99:45000 Loc:172.16.58.99:45000 T:5 S:ESTAB *
```

```
Audit Rule Configuration
Audit name AUDIT.1
  info actions alarm
  attack actions alarm drop reset
```

You can verify which interfaces have audit rules applied to them with the **show ip audit interface** command (see Example 2).

Example 2 Output from show ip audit interface Command

```
ids2611#show ip audit interface
Interface Configuration
Interface Ethernet0
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
    attack actions alarm drop reset
  Outgoing IDS audit rule is not set
Interface Ethernet1
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
    attack actions alarm drop reset
  Outgoing IDS audit rule is not set
```

Configuration Examples

This section provides the following configuration examples:

- Cisco IOS IDS Reporting to Two Directors
- Adding an ACL to the Audit Rule
- Disabling a Signature
- Adding an ACL to Signatures
- Dual-Tier Signature Response

Cisco IOS IDS Reporting to Two Directors

In the following example, Cisco IOS IDS is initialized. Notice that the router is reporting to two Directors, one of which has been configured with two routes for communication. Also notice that the AUDIT.1 audit rule will apply both info and attack signatures:

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2
ip audit po remote hostid 15 orgid 123 rmtaddress 10.1.2.99 localaddress 10.1.1.1

ip audit name AUDIT.1 info action alarm
ip audit name AUDIT.1 attack action alarm drop reset

interface e0
 ip address 10.1.1.1 255.0.0.0
 ip audit AUDIT.1 in

interface e1
 ip address 172.16.57.1 255.255.255.0
 ip audit AUDIT.1 in
```

Adding an ACL to the Audit Rule

In the following example, an ACL is added to account for a NetSonar device (172.16.59.16) that scans for all types of attacks. As a result, no packets originating from the device will be audited:

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2
ip audit po remote hostid 15 orgid 123 rmtaddress 10.1.2.99 localaddress 10.1.1.1

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop reset

interface e0
 ip address 10.1.1.1 255.0.0.0
 ip audit AUDIT.1 in

interface e1
 ip address 172.16.57.1 255.255.255.0
 ip audit AUDIT.1 in

access-list 90 deny 172.16.59.16
access-list 90 permit any
```

Disabling a Signature

The security administrator notices that the router is generating a lot of false positives for signatures 1234, 2345, and 3456. The system administrator knows that there is an application on the network that is causing signature 1234 to fire, and it is not an application that should cause security concerns. This signature can be disabled, as illustrated in the following example:

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2
ip audit po remote hostid 15 orgid 123 rmtaddress 10.1.2.99 localaddress 10.1.1.1

ip audit signature 1234 disable

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop reset

interface e0
 ip address 10.1.1.1 255.0.0.0
 ip audit AUDIT.1 in

interface e1
 ip address 172.16.57.1 255.255.255.0
 ip audit AUDIT.1 in

access-list 90 deny 172.16.59.16
access-list 90 permit any
```

Adding an ACL to Signatures

After further investigation, the security administrator discovers that the false positives for signatures 2345 and 3456 are caused by specific applications on hosts 10.4.1.1 and 10.4.1.2, as well as by some workstations using DHCP on the 172.16.58.0 subnet. Attaching an ACL that denies processing of these hosts stops the creation of false positive alarms, as illustrated in the following example:

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2
ip audit po remote hostid 15 orgid 123 rmtaddress 10.1.2.99 localaddress 10.1.1.1

ip audit signature 1234 disable
ip audit signature 2345 list 91
ip audit signature 3456 list 91

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm drop reset

interface e0
 ip address 10.1.1.1 255.0.0.0
 ip audit AUDIT.1 in

interface e1
 ip address 172.16.57.1 255.255.255.0
 ip audit AUDIT.1 in

access-list 90 deny 172.16.59.16
access-list 90 permit any
access-list 91 deny host 10.4.1.1
access-list 91 deny host 10.4.1.2
access-list 91 deny 172.16.58.0 0.0.0.255
access-list 91 permit any
```

Dual-Tier Signature Response

The company has now reorganized and has placed only trusted people on the 172.16.57.0 network. The work done by the employees on these networks must not be disrupted by Cisco IOS IDS, so attack signatures in the AUDIT.1 audit rule now will only alarm on a match.

For sessions that originate from the outside network, any attack signature matches (other than the false positive ones that are being filtered out) are to be dealt with in the following manner: send an alarm, drop the packet, and reset the TCP session.

This dual-tier method of signature response is accomplished by configuring two different audit specifications and applying each to a different ethernet interface, as illustrated in the following example:

```
ip audit smtp spam 25
ip audit notify nr-director
ip audit notify log
ip audit po local hostid 55 orgid 123
ip audit po remote hostid 14 orgid 123 rmtaddress 10.1.1.99 localaddress 10.1.1.1
preference 1
ip audit po remote hostid 14 orgid 123 rmtaddress 172.16.58.99 localaddress 10.2.1.1
preference 2
ip audit po remote hostid 15 orgid 123 rmtaddress 10.1.2.99 localaddress 10.1.1.1

ip audit signature 1234 disable
ip audit signature 2345 list 91
ip audit signature 3456 list 91

ip audit name AUDIT.1 info list 90 action alarm
ip audit name AUDIT.1 attack list 90 action alarm
ip audit name AUDIT.2 info action alarm
ip audit name AUDIT.2 attack alarm drop reset

interface e0
 ip address 10.1.1.1 255.0.0.0
 ip audit AUDIT.2 in

interface e1
 ip address 172.16.57.1 255.255.255.0
 ip audit AUDIT.1 in

access-list 90 deny host 172.16.59.16
access-list 90 permit any
access-list 91 deny host 10.4.1.1
access-list 91 deny host 10.4.1.2
access-list 91 deny 172.16.58.0 0.0.0.255
access-list 91 permit any
```

Command Reference

This section documents the following Cisco IOS IDS commands:

- clear ip audit configuration
- clear ip audit statistics
- ip audit
- ip audit attack
- ip audit info
- ip audit name
- ip audit notify
- ip audit po local
- ip audit po max-events
- ip audit po protected
- ip audit po remote
- ip audit signature
- ip audit smtp
- show ip audit statistics
- show ip audit configuration
- show ip audit debug
- show ip audit interface

In Cisco IOS Release 12.0(1)T or later, you can search and filter the output for **show** and **more** commands. This functionality is useful when you need to sort through large amounts of output, or if you want to exclude output that you do not need to see.

To use this functionality, enter a **show** or **more** command followed by the “pipe” character (`|`), one of the keywords **begin**, **include**, or **exclude**, and an expression that you want to search or filter on:

```
command / {begin | include | exclude} regular-expression
```

Following is an example of the **show atm vc** command in which you want the command output to begin with the first line where the expression “PeakRate” appears:

```
show atm vc / begin PeakRate
```

For more information on the search and filter functionality, refer to the Cisco IOS Release 12.0(1)T feature module titled *CLI String Search*.

clear ip audit configuration

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

clear ip audit configuration

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

Examples

The following example clears the existing IP audit configuration:

```
clear ip audit configuration
```

clear ip audit statistics

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

clear ip audit statistics

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

Examples

The following example clears all IP audit statistics:

```
clear ip audit statistics
```

ip audit

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

```
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.

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

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

```
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	Send an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.
drop	Drop the packet. Used with the action keyword.
reset	Reset 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.

Examples

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

```
ip audit attack action alarm drop reset
```

ip audit info

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

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	Send an alarm to the console, NetRanger Director, or to a syslog server. Used with the action keyword.
drop	Drop the packet. Used with the action keyword.
reset	Reset 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.

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

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

```
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	Specifies an ACL to attach to the audit rule.
<i>standard-acl</i>	Integer representing an access control list. Use with the list keyword.
action	Specifies an action or actions to take in response to a match.
alarm	Send an alarm to the console, NetRanger Director, or to a syslog server. Use with the action keyword.
drop	Drop the packet. Use with the action keyword.
reset	Reset 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

Use the **ip audit notify** global configuration command to specify the methods of event notification. Use the **no** form of this command to disable event notifications.

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.

Refer to the "Message Formats" section of this document for more information on NetRanger Post Office and syslog message formats.

Examples

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

Command	Description
ip audit po remote	Sets IP address for remote NetRanger Director.
ip audit po local	Sets IP address for the Cisco IOS IDS router.

ip audit po local

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. Use the **no** form of this command to set the local Post Office parameters to their default settings.

ip audit po local **hostid** *host-id* **orgid** *org-id*

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

Syntax Description

hostid <i>host-id</i>	Specifies a NetRanger host ID. Unique integer in the range 1-65535 used in NetRanger communications to identify the local host. Use with the hostid keyword.
orgid <i>org-id</i>	Specifies a NetRanger organization ID. 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.

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

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

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

no ip audit po max-events

Syntax Description

number-of-events

Integer in the range of 1–65535 that designates the maximum number of events allowable in the event queue. Use with the **max-events** keyword.

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

Use the **ip audit po protected** global configuration command to specify whether an address is on a protected network. Use the **no** form of this command to remove network addresses from the protected network list. 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	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 belong 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

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

```
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

hostid	Specifies a NetRanger host ID.
<i>host-id</i>	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>org-id</i>	Unique integer in the range 1-65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the orgid keyword.
rmtaddress	Specifies the IP address of the NetRanger Director.
localaddress	Specifies the IP address of the Cisco IOS IDS router.
<i>ip-address</i>	IP address of the NetRanger Director or Cisco IOS IDS router's interface. Use with the rmtaddress and localaddress keywords.
port	Specifies a UDP port through which to send messages.
<i>port-number</i>	Integer representing the UDP port on which the Director is listening for event notifications. Use with the port keyword.
preference	Specifies a route preference for communication.
<i>preference-number</i>	Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the preference keyword.
timeout	Specifies a timeout value for Post Office communications.
<i>seconds</i>	Integer representing the heartbeat timeout value for Post Office communications. Use with the timeout keyword.
application	Specifies the type of application that is receiving the Cisco IOS IDS messages.
director	Specifies that the receiving application is the NetRanger Director interface.
logger	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 Director. In this case, use the **ip audit po remote** command to add each Director to which the router sends notifications.

More than one route can be established to the same 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 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

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

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. Use the **no** version of this command to set the number of recipients to the default setting.

ip audit smtp spam *number-of-recipients*

no ip audit smtp spam

Syntax Description

spam	Specifies a threshold beyond which the Cisco IOS 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.

Defaults

The default number of recipients is 250.

Command Modes

Global configuration

Command History

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

Examples

In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```

show ip audit statistics

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

show ip audit statistics

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

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

You can use the master indexes or search online to find documentation of related commands.

Command	Description
clear ip audit statistics	Resets all IP audit statistics.

show ip audit configuration

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.

show ip audit configuration

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

Examples

The following example displays the output of the **show ip audit statistics** 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

You can use the master indexes or search online to find documentation of related commands.

Command	Description
clear ip audit statistics	Resets all IP audit statistics.

show ip audit debug

Use the **show ip audit debug** EXEC command to display the enabled debug flags.

show ip audit debug

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

Examples

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

```
IDS Function Trace debugging is on
IDS Object Creations debugging is on
IDS Object Deletions debugging is on
```

show ip audit interface

Use the **show ip audit interface** EXEC command to display the interface configuration.

show ip audit interface

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

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

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
```

Message Formats

This section describes the following topics:

- NetRanger Post Office Format
- Syslog Format

NetRanger Post Office Format

Messages sent to the NetRanger Director are sent in the NetRanger Post Office format. Each line of a NetRanger Post Office message is a comma-delimited string that provides information on the alarm generated. The NetRanger Director converts this information into an alarm on the Director's GUI.

For more information on the NetRanger Post Office format, refer to the *NetRanger User Guide*.

Syslog Format

Syslog messages are colon-delimited strings with the following format:

```
Sig:Sig-Number:Sig-name from Source-IP to Destination-IP
```

where *Sig-Number* is the signature's number, as defined in the NetRanger Network Security Database; *Sig-Name* is the name of the signature; *Source-IP* is the source's IP address; and *Destination-IP* is the destination's IP address.

For example:

```
Sig:1000:Bad IP Option List from %i to %i  
Sig:1001:IP options-Record Packet Route from %i to %i
```

Cisco IOS IDS Signature List

The following is a complete list of Cisco IOS IDS signatures. The signatures are listed in numerical order by their signature number in the NetRanger Network Security Database. After each signature's name is an indication of the type of signature it is (Info or Attack, Atomic or Compound).

The intrusion-detection signatures included in the new release of the Cisco IOS Firewall were chosen from a broad cross-section of intrusion-detection signatures as representative of the most common network attacks and information-gathering scans that are not commonly found in an operational network.

Note Atomic signatures that have an asterisked Atomic (Atomic*) are allocated memory for session states by CBAC.

1000 IP options-Bad Option List (Info, Atomic)

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 IP options-Record Packet Route (Info, Atomic)

Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 7 (Record Packet Route).

1002 IP options-Timestamp (Info, Atomic)

Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 4 (Timestamp).

1003 IP options-Provide s,c,h,tcc (Info, Atomic)

Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 2 (Security options).

1004 IP options-Loose Source Route (Info, Atomic)

Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 3 (Loose Source Route).

1005 IP options-SATNET ID (Info, Atomic)

Triggers on receipt of an IP datagram where the IP option list for the datagram includes option 8 (SATNET stream identifier).

1006 IP options-Strict Source Route (Info, Atomic)

Triggers on receipt of an IP datagram in which the IP option list for the datagram includes option 2 (Strict Source Routing).

1100 IP Fragment Attack (Attack, Atomic)

Triggers when any IP datagram is received with the "more fragments" flag set to 1 or if there is an offset indicated in the offset field.

1101 Unknown IP Protocol (Attack, Atomic)

Triggers when an IP datagram is received with the protocol field set to 101 or greater. These protocol types are undefined or reserved and should not be used.

1102 Impossible IP Packet (Attack, Atomic)

This triggers when an IP packet arrives with source equal to destination address. This signature will catch the so-called Land Attack.

2000 ICMP Echo Reply (Info, Atomic)

Triggers when a IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 0 (Echo Reply).

2001 ICMP Host Unreachable (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 3 (Host Unreachable).

2002 ICMP Source Quench (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 4 (Source Quench).

2003 ICMP Redirect (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 5 (Redirect).

2004 ICMP Echo Request (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 8 (Echo Request).

2005 ICMP Time Exceeded for a Datagram (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 11 (Time Exceeded for a Datagram).

2006 ICMP Parameter Problem on Datagram (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 12 (Parameter Problem on Datagram).

2007 ICMP Timestamp Request (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 13 (Timestamp Request).

2008 ICMP Timestamp Reply (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 14 (Timestamp Reply).

2009 ICMP Information Request (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 15 (Information Request).

2010 ICMP Information Reply (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 16 (ICMP Information Reply).

2011 ICMP Address Mask Request (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 17 (Address Mask Request).

2012 ICMP Address Mask Reply (Info, Atomic)

Triggers when an IP datagram is received with the “protocol” field in the IP header set to 1 (ICMP) and the “type” field in the ICMP header set to 18 (Address Mask Reply).

2150 Fragmented ICMP Traffic (Attack, Atomic)

Triggers when an IP datagram is received with the protocol field in 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 Large ICMP Traffic (Attack, Atomic)

Triggers when an IP datagram is received with the protocol field in the IP header set to 1 (ICMP) and the IP length is greater than 1024.

2154 Ping of Death Attack (Attack, Atomic)

Triggers when an IP datagram is received with the protocol field in the IP header set to 1 (ICMP), the Last Fragment bit is set, and

```
( IP offset * 8 ) + ( IP data length ) > 65535
```

In other words, 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 TCP - no bits set in flags (Attack, Atomic)

Triggers when a TCP packet is received with no bits set in the flags field.

3041 TCP - SYN and FIN bits set (Attack, Atomic)

Triggers when a TCP packet is received with both the SYN and FIN bits set in the flag field.

3042 TCP - FIN bit with no ACK bit in flags (Attack, Atomic)

Triggers when a TCP packet is received with the FIN bit set but with no ACK bit set in the flags field.

3050 Half-open SYN Attack/SYN Flood (Attack, Compound)

Triggers when multiple TCP sessions have been improperly initiated on any of several well-known service ports. Detection of this signature is currently limited to FTP, Telnet, HTTP, and e-mail servers (TCP ports 21, 23, 80, and 25 respectively).

3100 Smail Attack (Attack, Compound)

Triggers on the very common "smail" attack against SMTP-compliant e-mail servers (frequently sendmail).

3101 Sendmail Invalid Recipient (Attack, Compound)

Triggers on any mail message with a "pipe" (|) symbol in the recipient field.

3102 Sendmail Invalid Sender (Attack, Compound)

Triggers on any mail message with a "pipe" (|) symbol in the "From:" field.

3103 Sendmail Reconnaissance (Attack, Compound)

Triggers when "expn" or "vrfy" commands are issued to the SMTP port.

3104 Archaic Sendmail Attacks (Attack, Compound)

Triggers when "wiz" or "debug" commands are issued to the SMTP port.

3105 Sendmail Decode Alias (Attack, Compound)

Triggers on any mail message with ": decode@" in the header.

3106 Mail Spam (Attack, Compound)

Counts number of Rcpt to: lines in a single mail message and alarms after a user-definable maximum has been exceeded (default is 250).

3107 Majordomo Execute Attack (Attack, Compound)

A bug in the Majordomo program will allow remote users to execute arbitrary commands at the privilege level of the server.

3150 FTP Remote Command Execution (Attack, Compound)

Triggers when someone tries to execute the FTP SITE command.

3151 FTP SYST Command Attempt (Info, Compound)

Triggers when someone tries to execute the FTP SYST command.

3152 FTP CWD ~root (Attack, Compound)

Triggers when someone tries to execute the CWD ~root command.

3153 FTP Improper Address Specified (Attack, Atomic*)

Triggers if a port command is issued with an address that is not the same as the requesting host.

3154 FTP Improper Port Specified (Attack, Atomic*)

Triggers if a port command is issued with a data port specified that is less than 1024 or greater than 65535.

4050 UDP Bomb (Attack, Atomic)

Triggers when the UDP length specified is less than the IP length specified.

4100 Tftp Passwd File (Attack, Compound)

Triggers on an attempt to access the passwd file (typically /etc/passwd) via TFTP.

6100 RPC Port Registration (Info, Atomic*)

Triggers when attempts are made to register new RPC services on a target host.

6101 RPC Port Unregistration (Info, Atomic*)

Triggers when attempts are made to unregister existing RPC services on a target host.

6102 RPC Dump (Info, Atomic*)

Triggers when an RPC dump request is issued to a target host.

6103 Proxied RPC Request (Attack, Atomic*)

Triggers when a proxied RPC request is sent to the portmapper of a target host.

6150 ypserv Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the YP server daemon (ypserv) port.

6151 ypbind Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the YP bind daemon (ypbind) port.

6152 yppasswdd Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the YP password daemon (yppasswdd) port.

6153 ypupdated Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the YP update daemon (ypupdated) port.

6154 ypxfrd Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the YP transfer daemon (ypxfrd) port.

6155 mountd Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the mount daemon (mountd) port.

6175 rexd Portmap Request (Info, Atomic*)

Triggers when a request is made to the portmapper for the remote execution daemon (rex) port.

6180 rexd Attempt (Info, Atomic*)

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 statd Buffer Overflow (Attack, Atomic*)

Triggers when a large statd request is sent. This could be an attempt to overflow a buffer and gain access to system resources.

8000 FTP Retrieve Password File (Attack, Atomic*)

SubSig ID: 2101

Triggers on string "passwd" issued during an FTP session. May indicate someone attempting to retrieve the password file from a machine in order to crack it and gain unauthorized access to system resources.

Glossary

The following terms are used in this document:

attack signature—A signature that detects attacks attempted into the protected network, such as denial of service attempts or the execution of illegal commands during an FTP session.

atomic signature—Atomic signatures can detect patterns as simple as an attempt to access a specific port on a specific host.

compound signature—Compound signatures can detect complex patterns, such as a sequence of operations distributed across multiple hosts over an arbitrary period of time.

info signature—A signature that detects information-gathering activity, such as a port sweep.

intrusion detection—Intrusion detection involves the ongoing monitoring of network traffic for potential misuse or policy violations. It matches network traffic against lists of signatures, which look for patterns of misuse.

NetRanger Director—The Director is NetRanger's graphical control interface. A single Director can manage and monitor a group of Sensors, which enables security personnel to secure a network from a centralized console.

NetRanger Sensor—The NetRanger Sensor is an intrusion detection appliance that analyzes network traffic, using signatures to search for signs of unauthorized activity.

signature—A signature detects patterns of misuse in network traffic. In Cisco IOS IDS, signatures are categorized into four types: Info Atomic, Info Compound, Attack Atomic, or Attack Compound. For a complete listing of Cisco IOS IDS signatures, refer to the "Cisco IOS IDS Signature List" section of this document.