# IDS Configuration

etutorials.org/Networking/Router+firewall+security/Part+VII+Detecting+and+Preventing+Attacks/Chapter+16.+Intrusion-Detection+System/IDS+Configuration/

This section discusses how to set up and verify the operation of IDS. The configuration process requires three steps:

**Step 1.** Initialization configuration

**Step 2.** Logging or PostOffice configuration

**Step 3.** Audit rule configuration and activation

The following sections cover these three steps, as well as how to verify the operation of IDS.

### Step 1: Initialization Configuration

You can configure two basic initialization commands for IDS:

```
Router(config)# ip audit po max-events
#_of_events

Router(config)# ip audit smtp spam
#_of_recipients
```

The ip audit po max-events command limits the number of IDS events that the Cisco IOS queues up to send to a remote device. By default, this is 250 events, but this can range from 1 to 65,535. This limit is used to ensure that if a hacker tried to flood a router with a lot of attacks, the router would not overload itself in trying to process all of them. Otherwise, this basically would allow the hacker to create a DoS attack against the router itself.

The ip audit smtp spam command is used to limit e-mail spamming that uses mass mailings. With this command, the default number of recipients allowed in an e-mail message is 250. If an e-mail message contains more than this value, the router takes the configured action (I discuss these actions later in the "Global Policies" and "Specific Policies" sections). The number of recipients can range from 1 to 65,535.

### Step 2: Logging and PostOffice Configuration

The Cisco IOS can use two methods when logging IDS events: log the information using syslog or log the information using an IDS Director. Using syslog, the Cisco IOS can log information locally (the console or the internal buffer) or remotely (a syslog server). If you want to use the syslog method, you must configure the following IDS statement:

```
Router(config)# ip audit notify
log
```

This is the default. If you are using CiscoWorks VMS with Security Monitoring Center (MC), you can forward the router's syslog messages to Security MC, which is used to centralize the repository and reporting of alarm information. When logging informational signatures to the router's console, you also need to execute the following command:

```
Router(config)# logging console
info
```

Other methods of using syslog are discussed in Chapter 18, "Logging Events."

Your second logging option is to log information to an IDS Director, which can include Cisco's IDS management console as well as a 4200 series sensor running 3.x. This is more difficult to set up because the IDS Director uses a Cisco-proprietary communication protocol called PostOffice. This protocol defines how an agent and management console, as well as two agents, share information with each other. To set up IDS Director communications, use the following syntax:

```
Router(config)# ip audit notify nr-director

Router(config)# ip audit po local hostid host_ID orgid organization_ID



Router(config)# ip audit po remote hostid host_ID orgid organization_ID
rmtaddress

   IP_address localaddress IP_address [port port_#] [preference preference_#]

   [timeout seconds] [application {director | logger}]
```

The ip audit notify nr-director command enables the logging of IDS events to an IDS Director product. The ip audit po local command specifies the PostOffice configuration for the router; the ip audit po remote command specifies the configuration for the remote Director device.

With PostOffice, each device needs a unique combination of a host ID and an organization ID. The organization ID is used to group sensors. In smaller companies, normally only a single organization ID is necessary. For enterprise companies, you might have different organization IDs for each division, allowing for easier management of your sensor products. Within each organization, a device needs a unique host ID. This concept is similar to IP addressing, in which you have network numbers and hosts within a network. Both of these IDs range from 1 to 65,535.

For the ip audit po local command, you must specify the router's personal ID numbers for the host and organization values. Likewise, you must specify the Director's PostOffice ID information in the ip audit po remote command. However, unlike the router's PostOffice configuration, you have to tell your router many more things about the remote Director in the ip audit po remote command. After specifying the PostOffice ID of the Director, you need to specify the IP address of the Director and then the IP address that the router will use as its source address (an address on one of its physical or loopback interfaces). The rest of the parameters are optional:

- port? By default, PostOffice uses UDP port 45,000, but you can change this (if you do, you also must change it on your other Director and sensor products).
- preference? This prioritizes multiple statements, with different IP addresses, for the same Director. The default preference is 1 (highest). Assign the primary addresses a preference of 1; assign secondary addresses a lower preference number.
- timeout? This determines the number of seconds that the router waits for the PostOffice reply to be received. The default is 5 seconds.
- application? You can specify two application types: director (default) or logger. With the director method,

the Cisco IOS uses PostOffice to send IDS messages to a Director product (management platform). This then shows up as an alarm in the management console and also is logged in a file. With the logger method, the IDS messages are sent to a Cisco sensor product or to a Director?with either method, only a log message is recorded. Normally, you use this method if you are not using Cisco's Director product for management, but you have Cisco sensors and want to centralize your logging information. Of course, you also easily can do this with syslog.

NOTE

The router's PostOffice identifiers must be configured on the Director device to allow communication between the router and the Director. Also, any time you change the router's PostOffice ID information, you must save your configuration and reboot the router.

### Step 3: Audit Rule Configuration and Activation

When you have defined your logging method, you are ready to create your IDS auditing rules. Two sets of commands are used to configure audit rules: global (default actions) and specific.

### Global Policies

Global policies are used to take the appropriate actions for matching on signatures, unless a specific rule designates otherwise. To create your global policies, use these two commands:

```
Router(config)# ip audit info {action [alarm] [drop] [reset]}

Router(config)# ip audit attack {action [alarm] [drop] [reset]}
```

As you can see, the two commands specify actions for informational and attack signatures. Each has three possible actions that the router can take:

- alarm? Generate an alarm (log), where this is the default action
- drop? Drop the packet
- reset? For TCP connections, tear down the connection

These commands need to be configured only if you want to change the default action (alarm) and you want the Cisco IOS IDS engine to use the same policy for all traffic of the same signature category.

### Specific Policies

Besides globally changing the behavior or IDS, you can create specific IDS auditing policies. Typically, you do this if you have two interfaces on your router?perhaps one connected to the Internet and the other to a remote site?and you want to set up different IDS policies (actions to signature matches) for each interface. Here is the command syntax to set up your specific IDS auditing policies:

```
Router(config)# ip audit name audit_name {info | attack}

   [list standard_ACL_#_or_name] [action [alarm] [drop]
[reset]]
```

The first difference between this command and the two global commands is that you must give the policy a name. Following this, specify the signature category: either informational or attack. Optionally, you can specify a standard ACL number or name. With this option, only permit source IP address entries in the ACL are used for matching traffic. Remember my earlier warning: Using ACLs with IDS matching severely impacts the performance of the router. Following this are the actions for the specific policy. If you omit the action, it defaults to the action defined in the global policy.

### Signature Policies

By default, all signatures are enabled. In some cases, however, you want to disable one or multiple signatures, perhaps because of a high number of false positive matches. You can disable a signature with the following command syntax:

```
Router(config)# ip audit signature signature_#

   {disable | list standard_ACL_#_or_name}
```

You must specify the signature number that you want to disable. Signature numbers were discussed previously in Table 16-2. Following this, you specify one of two parameters. The disable parameter disables the signature for all IDS auditing policies on the router. The list parameter specifies a standard ACL. If a match on the signature occurs and the source IP address matches any of the deny entries in the standard ACL, the router takes no action; only permit entries will allow the router to perform the configured action for the IDS auditing policy. Again, remember my warning about performance issues when using ACLs with IDS policies.

Many IDS solutions enable you to trigger alarms on informational processes, such as pings or DNS zone transfers. This is useful if you have tight control over these things to begin with. However, if these are common occurrences in your network, it becomes much easier to hide a real attack by inserting it into a mass of false positives. I have run into this situation quite a few times, with administrators failing to tune their IDS solutions and receiving thousands of events to track on a daily basis. In some cases, the companies did not even know that they were under attack; in one case, the company already had been attacked successfully.

A good IDS solution brings important events to your immediate attention through a prioritization scheme. However, not all IDS solutions do this; in such cases, searching through lengthy log files for important events becomes difficult, if not impossible, if there are thousands of entries. Therefore, I highly recommend that you tune each IDS solution, disabling signatures that are not necessary or tuning profiles so that the number of false positives is reduced greatly.

### Protection Policies

When an IDS alarm is generated because a signature was triggered, the alarm contains a location designator for both the source and destination addresses. IN indicates that the address is internal to the network, and OUT indicates that it is external to the network. Of course, the router does not know internal from external: You must tell the router this. This is done with this configuration:

```
Router(config)# ip audit po protected IP_address [to
IP_address]
```

Any address specified in this command is listed as IN as a location designator in the alarm. You can specify a single address or a range of addresses (using the to parameter). Note that this command influences only the location tags placed in the alarm message and has no affect on the triggering of signatures.

### Policy Activation

After you have defined your IDS audit policies, you must activate them on an interface(s) before your router can use them. Use the following configuration to activate your IDS audit policies:

```
Router(config)# interface type [slot_#/]port_#

Router(config-if)# ip audit audit_name {in |
out}
```

You can specify that your policy be activated in the inbound or outbound direction on an interface. If you want to activate a policy in both directions, execute the command twice, specifying in for one command and out for the other. Normally, you activate your IDS policies inbound on a perimeter router's external interface. After you have activated your IDS policies, the router starts comparing packets to its signature database.

### IDS Verification

After you have set up IDS on your router, you can use one show command with multiple parameter options to test your IDS configuration:

```
Router(config)# show ip audit { all | configuration | interfaces |

   name audit_name | sessions | statistics}
```

The all parameter displays output from all of the other parameters (with the exception of sessions and statistics). The configuration parameter displays how you have configured IDS on your router. The interfaces parameter displays which interfaces do and do not have IDS policies activated on them. The name parameter displays the configuration of the specified audit policy. The sessions parameter displays IDS sessions (Director connections). The statistics parameter display statistics about the operation of IDS. Example 16-1 displays sample output with the all parameter.

### Example 16-1. Using the show ip audit all Command

```
Router# show ip audit all

Event notification through syslog is enabled
(1)

Event notification through Net Director is disabled

Default action(s) for info signatures is alarm
(2)

Default action(s) for attack signatures is alarm

Default threshold of recipients for spam signature is 250

PostOffice:HostID:0 OrgID:0 Msg dropped:0

          :Curr Event Buf Size:0  Configured:100

Post Office is not enabled - No connections are active
(3)

Audit Rule Configuration
(4)

 Audit name audit_ids

    attack actions alarm drop reset

Interface Configuration

 Interface FastEthernet0
(5)

  Inbound IDS audit rule is audit_ids

    attack actions alarm drop reset

  Outgoing IDS audit rule is not set
```

The following is an explanation of the output in Example 16-1, with reference to the numbering on the right side of the example:

1. Syslog is enabled and Director logging is disabled. These are the defaults.
2. These are the actions for the global policies. Notice that they are both set to alarm, which is the default.
3. PostOffice is not configured in this example.
4. This section contains your defined (specific) audit rules. In this example, only one specific policy has been defined: audit_ids. This policy enables only attack signatures, with a response of alarm, drop, and reset for matches on these signatures.
5. The audit_ids policy is enabled on FastEthernet0.

Example 16-2 displays sample output with the statistics parameter.

### Example 16-2. Using the show ip audit statistics Command

```
Router# show ip audit statistics

Signature audit statistics [process switch:fast switch]

  signature 1107 packets audited: [5:5]

  signature 2004 packets audited: [4:4]

  signature 2150 packets audited: [0:7]

Interfaces configured for audit 1

Session creations since subsystem startup or last reset 0

Current session counts (estab/half-open/terminating) [7:1:1]

Maxever session counts (estab/half-open/terminating)
[58:39:3]

Last session created never

Last statistic reset never


Post Office is not enabled - No connections are active
```

In this example, there were matches against three signatures. You also can see the number of packets processed and fast-switched (in the first set of brackets).

If you want to clear your IDS statistics, use the clear ip audit statistics command. If you want to clear the IDS configuration on your router completely, use the clear ip audit configuration command.