C H A P T E R 20

Configuring the NM CIDS

> **Note** The number of concurrent CLI sessions is limited based on the platform. The IDS 4215 and NM CIDS are limited to three concurrent CLI sessions. All other platforms allow ten concurrent sessions.

> **Note** The NM CIDS does not operate in inline mode, only in promiscuous mode, therefore you cannot configure intrusion prevention.

> **Note** The NM CIDS does not support virtualization. For more information on virtualization, see Configuring the Virtual Sensor, page 7-3.

> **Note** The NM CIDS does not support bridged interfaces. Although Cisco IOS allows you to configure IDS using the NM CIDS on a bridged interface, the NM CIDS is not designed to inspect traffic on bridged interfaces, and the configuration does not work.

This chapter describes the tasks you need to perform to set up the NM CIDS and get it ready to receive traffic. After that you are ready to configure intrusion detection. This chapter contains the following sections:

Configuration Sequence

Perform the following tasks to configure the NM CIDS:

1. Configure the IDS interfaces on the router.

2. Log in to the NM CIDS.

3. Initialize the NM CIDS.

   Run the **setup** command to initialize the NM CIDS.

4. Configure the NM CIDS to capture traffic for intrusion detection analysis.

5. Create the service account.

6. Perform the other initial tasks, such as adding users, trusted hosts, and so forth.

7. Configure intrusion detection.

8. Perform administrative tasks to keep your NM CIDS running smoothly.

9. Upgrade the IPS software with new signature updates and service packs.

10. Reimage the boot helper and bootloader when needed.

For More Information

- For the procedure for configuring the IDS interfaces on the router, see Configuring IDS-Sensor Interfaces on the Router, page 20-2.

- For the procedure for logging in to the NM CIDS, see Establishing the NM CIDS Sessions, page 20-4.

- For the procedure for using the setup command to initialize the NM CIDS, see Initializing NM CIDS, page 3-31.

- For the procedure for configuring the NM CIDS to capture traffic for intrusion detection analysis, see Configuring Packet Capture, page 20-5.

- For the procedure for creating service account, see Creating the Service Account, page 4-13.

- For the procedures for setting up the sensor, see Chapter 4, "Initial Configuration Tasks."

- For the procedures for configuring intrusion detection, see Chapter 9, "Configuring Anomaly Detection," Chapter 8, "Configuring Event Action Rules," Chapter 6, "Defining Signatures," and Chapter 13, "Configuring Attack Response Controller for Blocking and Rate Limiting."

- For the administrative procedures, see Chapter 16, "Administrative Tasks for the Sensor" and Administrative Tasks, page 20-7.

- For more information on obtaining the latest IPS software, see Obtaining Cisco IPS Software, page 22-1.

- For the procedures for reimaging the boot help and bootloader, see Installing the NM CIDS System Image, page 21-28.

Configuring IDS-Sensor Interfaces on the Router

The NM CIDS does not have an external console port. Console access to the NM CIDS is enabled when you issue the **service-module ids-module** *slot_number***/0 session** command on the router, or when you initiate a Telnet connection in to the router with the port number corresponding to the NM CIDS slot. The lack of an external console port means that the initial bootup configuration is possible only through the router.

When you issue the **service-module ids-sensor** *slot_number***/0 session** command, you create a console session with the NM CIDS, in which you can issue any IPS configuration commands. After completing work in the session and exiting the IPS CLI, you are returned to the Cisco IOS CLI.

The **session** command starts a reverse Telnet connection using the IP address of the ids-sensor interface. The ids-sensor interface is an interface between the NM CIDS and the router. You must assign an IP address to the ids-sensor interface before invoking the **session** command. Assigning a routable IP address can make the ids-sensor interface itself vulnerable to attacks. To counter that vulnerability, a loopback IP address is assigned to the ids-sensor interface.

To configure the NM CIDS interfaces, follow these steps:

Step 1 Enter privileged EXEC mode on the router.

```
router> enable
```

Step 2 Confirm the NM CIDS slot number in your router.

```
router # show interfaces ids-sensor slot_number/0
```

> **Note** You can also use the **show run** command. Look for "IDS-Sensor" and the slot number.

> **Note** Cisco IOS gives the NM CIDS the name "IDS-Sensor." In this example, 1 is the slot number and 0 is the port number, because there is only one port.

Step 3 Enable the CEF switching path.

```
router# configuration terminal
router(config)# ip cef
router(config)# exit
```

Step 4 Create a loopback interface.

```
router# configure terminal
router(config)# interface loopback 0
```

Step 5 Assign an IP address and netmask to the loopback interface.

```
router(config-if)# ip address 10.99.99.99 255.255.255.255
```

> **Note** You must assign an IP address to the internal interface of the NM CIDS to session in to the NM CIDS. Choose a network that does not overlap with any networks assigned to the other interfaces in the router.

Step 6 Assign an unnumbered loopback interface to the ids-sensor interface. Use slot 1 for this example.

```
router(config)# interface ids-sensor 1/0
router(config-if)# ip unnumbered loopback 0
```

Step 7 Activate the port.

```
router(config-if)# no shutdown
```

Step 8 Exit configuration mode.

```
router(config-if)# end
```

Step 9   Write the configuration to NVRAM.

```
router# write memory
Building configuration
[OK]
```

Establishing the NM CIDS Sessions

This section describes how to establish sessions between the router and the NM CIDS. It contains the following topics:

Sessioning to the NM CIDS

Use the **session** command to establish a session from the router to the NM CIDS. Press **Ctrl-Shift-6**, then **x**, to return a session prompt to a router prompt, that is, to go from the NM CIDS prompt back to the router prompt. Press **Enter** on a blank line to go back to the session prompt, the NM CIDS prompt. You should only suspend a session to the NM CIDS if you will be returning to the session after executing router commands. If you do not plan on returning to the NM CIDS session, you should close the session rather than suspend it.

When you close a session, you are logged completely out of the NM CIDS CLI and a new session connection requires a username and password to log in. A suspended session leaves you logged in to the CLI. When you connect with the **session** command, you can go back to the same CLI without having to provide your username and password.

Note   Telnet clients vary. In some cases, you may have to press **Ctrl-6 + x**. The control character is specified as ^^, Ctrl-^, or ASCII value 30 (hex 1E).

Caution   If you use the **disconnect** command to leave the session, the session remains running. The open session can be exploited by someone wanting to take advantage of a connection that is still in place.

To open and close sessions to the NM CIDS, follow these steps:

Step 1   Open a session from the router to the NM CIDS.

```
router# service-module ids-sensor 1/0 session
Trying 10.99.99.99, 2033 ... Open
```

Step 2   Exit the NM CIDS session.

```
nm-cids# exit
```

Note   If you are in submodes of the IPS CLI, you must exit all submodes. Type **exit** until the sensor login prompt appears.

Failing to close a session properly makes it possible for others to exploit a connection that is still in place. Remember to type **exit** at the `Router#` prompt to close the Cisco IOS session completely.

Step 3 Suspend and close the session to the NM CIDS by pressing **Ctrl-Shift** and pressing **6**. Release all keys, and then press **x**.

> **Note** When you are finished with a session, you need to return to the router to establish the association between a session (the IPS application) and the router interfaces you want to monitor.

Step 4 Disconnect from the router.

```
router# disconnect
```

Step 5 Press **Enter** to confirm the disconnection.

```
router# Closing connection to 10.99.99.99 [confirm] <Enter>
```

Telneting to the NM CIDS

You can also Telnet directly to the router with the port number corresponding to the NM CIDS slot. Use the address you established when configuring the loopback 0 interface.

The port number is determined by the following formula: 2001 + 32 x slot number.

For example, for slot 1, the port number is 2033, for slot 2, it is 2065, and so forth.

To use Telnet to invoke a session to port 2033:

```
router# telnet 10.99.99.99 2033
```

For More Information

For the procedure for configuring the loopback 0 interface, see Configuring IDS-Sensor Interfaces on the Router, page 20-2.

Configuring Packet Capture

You must enable the desired interfaces (including subinterfaces) on the router for packet monitoring. You can select any number of interfaces or subinterfaces to be monitored. The packets sent and received on these interfaces are forwarded to the NM CIDS for inspection. You enable and disable the interfaces through the router CLI (Cisco IOS).

> **Note** If the router is performing encryption, the NM CIDS receives the packets after decryption coming in to the router and before encryption leaving the router.

To configure packet capture on the NM CIDS, follow these steps:

Step 1 Log in to the router console.

Step 2 View your interface configuration.

```
router# show run
```

Step 3   Identify the interfaces or subinterfaces that you want to monitor, for example, FastEthernet0/0.

> **Note**   You can choose more than one interface or subinterface to monitor, but you can only edit one interface at a time.

Step 4   Enter global configuration mode.

```
router# configure terminal
```

Step 5   Specify the interface or subinterface.

```
router(config)# interface FastEthernet0/0
```

> **Note**   The traffic comes from one of the router interfaces.

Step 6   Configure the interface to copy network traffic to the NM CIDS.

```
router(config-if)# ids-service-module monitoring
```

> **Note**   Use the **no ids-service-module monitoring** command to turn off monitoring.

Step 7   Exit interface mode.

```
router(config-if)# exit
```

Step 8   Repeat Steps 3 though 6 for each interface or subinterface that you want to monitor.

Step 9   Exit global configuration mode.

```
router(config)# exit
```

Step 10   Verify that the NM CIDS is analyzing network traffic.

a.   Open a Telnet or SSH session to the external interface on the NM CIDS, or establish a router console session.

> **Note**   SSH requires allowed hosts.

b.   Log in to the NM CIDS.

c.   View the interface statistics to make sure the monitoring interface is up.

```
nm-cids# show interface clear
nm-cids# show interface
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 23
   Total Bytes Received = 1721
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
```

```
        Total Jumbo Packets Received = 0
        Total Undersize Packets Received = 0
        Total Receive Errors = 0
        Total Receive FIFO Overruns = 0
        Total Packets Transmitted = 2
        Total Bytes Transmitted = 120
        Total Multicast Packets Transmitted = 0
        Total Broadcast Packets Transmitted = 0
        Total Jumbo Packets Transmitted = 0
        Total Undersize Packets Transmitted = 0
        Total Transmit Errors = 0
        Total Transmit FIFO Overruns = 0
```

d. Repeat Step c to see the counters gradually increasing. This indicates that the NM CIDS is receiving network traffic.

If the counters are not increasing, make sure the you executed Steps 3 though 6 properly and that FastEthernet0/1 was added to the virtual sensor when you initialized the NM CIDS with the **setup** command.

For More Information

For the procedure for adding SSH allowed hosts, see Adding Hosts to the SSH Known Hosts List, page 4-31.

Administrative Tasks

The following section describes how to reboot the NM CIDS and how to check the status of the Cisco IPS software. It contains the following topics:

- Shutting Down, Reloading, and Resetting the NM CIDS, page 20-7
- Checking the Status of the Cisco IPS Software, page 20-8

Shutting Down, Reloading, and Resetting the NM CIDS

The Cisco IOS provides the following commands to control the NM CIDS: **shutdown**, **reload**, and **reset**:

- **shutdown**—Brings the operating system down gracefully:

```
router# service-module ids-sensor slot_number/0 shutdown
```

⚠️
Caution   Make sure you execute a **shutdown** command before you remove the NM CIDS from the router. Failing to do so can lead to the loss of data or the corruption of the hard-disk drive.

- **reload**—Performs a graceful halt and reboot of the operating system on the NM CIDS:

```
router# service-module ids-sensor slot_number/0 reload
```

- **reset**—Resets the hardware on the NM CIDS. Typically this command is used to recover from a shutdown.

```
router# service-module ids-sensor slot_number/0 reset
```

The following warning appears:

```
router# service-module ids-sensor 1/0 reset
Use reset only to recover from shutdown or failed state
Warning: May lose data on the hard disc!
Do you want to reset?[confirm]
```

⚠

Caution   Hard-disk drive data loss only occurs if you issue the **reset** command without first shutting down the NM CIDS. If the NM CIDS is still running correctly, use the **reload** command rather than the **reset** command. You can use the **reset** command safely in other situations.

Checking the Status of the Cisco IPS Software

Use the **status** command to check the status of the Cisco IPS software running on the router:

```
router# service-module ids-sensor slot_number/0 status
```

Something similar to the following output appears:

```
Router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor 1/0
Service Module supports session via TTY line 33
Service Module is in Steady state
Getting status from the Service Module, please wait..
Service Module Version information received,
Major ver = 1, Minor ver= 1
Cisco Systems Intrusion Detection System Network Module
Software version: 5.0(1)S42
Model: NM-CIDS
Memory: 254676 KB
Mgmt IP addr:     xx.xx.xx.xx
Mgmt web ports:    443
Mgmt TLS enabled: true
```

Supported Cisco IOS Commands

The **service-module ids-sensor** *slot_number/*0 Cisco IOS command is new to support the NM CIDS. The slot number can vary, but the port is always 0.

The following options apply:

- Privileged mode EXEC

    – **service-module ids-sensor** *slot_number/*0 **reload**

    Reloads the operating system on the NM CIDS.

    – **service-module ids-sensor** *slot_number/*0 **reset**

    Provides a hardware reset to the NM CIDS.

    – **service-module ids-sensor** *slot_number/*0 **session**

    The **session** command lets you access the IPS console.

– **service-module ids-sensor** *slot_number/***0 shutdown**

Shuts down the IPS applications running on the NM CIDS.

⚠

Caution   Removing the NM CIDS without proper shutdown can result in the hard-disk drive being corrupted. After successful shutdown of the NM CIDS applications, Cisco IOS prints a message indicating that you can now remove the NM CIDS.

– **service-module ids-sensor** *slot_number/***0 status**

Provides information on the status of the Cisco IPS software.

• Configure interfaces mode `(config-if)`

– **ids-service-module monitoring**

You can enable IPS monitoring on a specified interface (or subinterface). Both inbound and outbound packets on the specified interface are forwarded for monitoring.