



# CHAPTER 16

## Configuring NM-CIDS

---

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



### Note

---

NM-CIDS does not operate in inline mode, only in promiscuous mode, therefore you cannot configure intrusion prevention.

---

This chapter contains the following sections:

- [Configuration Sequence, page 16-1](#)
- [Configuring IDS-Sensor Interfaces on the Router, page 16-2](#)
- [Establishing NM-CIDS Sessions, page 16-3](#)
- [Configuring Packet Capture, page 16-5](#)
- [Administrative Tasks for NM-CIDS, page 16-7](#)
- [Supported Cisco IOS Commands, page 16-8](#)

## Configuration Sequence

Perform the following tasks to configure NM-CIDS:

1. Configure the IDS interfaces on the router.  
For the procedure, see [Configuring IDS-Sensor Interfaces on the Router, page 16-2](#).
2. Log in to NM-CIDS.  
For the procedure, see [Establishing NM-CIDS Sessions, page 16-3](#).
3. Initialize NM-CIDS.  
Run the **setup** command to initialize NM-CIDS.  
For the procedure, see [Chapter 3, “Initializing the Sensor.”](#)
4. Configure NM-CIDS to capture traffic for intrusion detection analysis.  
For the procedure, see [Configuring Packet Capture, page 16-5](#).
5. Create the service account.  
A service account is needed for password recovery and other special debug situations directed by TAC.

For the procedure, see [Creating the Service Account, page 4-13](#).



### Caution

You should carefully consider whether you want to create a service account. The service account provides shell access to the system, which makes the system vulnerable. However, you can use the service account to create a new password if the Administrator password is lost. Analyze your situation to decide if you want a service account existing on the system.

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

For the procedures, see [Chapter 4, “Initial Configuration Tasks.”](#)

7. Configure intrusion detection.

For the procedures, see [Chapter 6, “Configuring Event Action Rules,”](#) [Chapter 7, “Defining Signatures,”](#) and [Chapter 10, “Configuring Blocking.”](#)

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

For the procedures, see [Chapter 13, “Administrative Tasks for the Sensor,”](#) and [Administrative Tasks for NM-CIDS, page 16-7](#).

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

For more information, see [Obtaining Cisco IPS Software, page 18-1](#).

10. Reimage the boot helper and bootloader when needed.

For the procedures, see [Installing the NM-CIDS System Image, page 17-19](#).

## Configuring IDS-Sensor Interfaces on the Router

NM-CIDS does not have an external console port. Console access to 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 into 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 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 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 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** 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 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 2** Enable the CEF switching path:

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

**Step 3** Create a loopback interface:

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

**Step 4** Assign an IP address and netmask to the loopback interface:

```
router(config-if)# ip address 10.16.0.0 255.255.0.0
```



**Note** You must assign an IP address to the NM-CIDS’s internal interface to session in to NM-CIDS. Choose a network that does not overlap with any networks assigned to the other interfaces in the router. It does not have to be a real IP address, because you will not be using this address to access NM-CIDS.

**Step 5** 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 6** Activate the port:

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

**Step 7** Exit configuration mode:

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

**Step 8** Write the configuration to NVRAM:

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

## Establishing NM-CIDS Sessions

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

- [Sessioning to NM-CIDS, page 16-4](#)
- [Telneting to NM-CIDS, page 16-5](#)

## Sessioning to NM-CIDS

Use the **session** command to establish a session from the router to 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 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 NM-CIDS, follow these steps:

**Step 1** Open a session from the router to NM-CIDS:

```
router# service-module ids-sensor 1/0 session  
Trying 10.16.0.0, 2033 ... Open
```

**Step 2** Press **Ctrl-Shift-6** and then **x** to return to the router prompt and to suspend the NM-CIDS session.

**Step 3** Press **Enter** on a blank line to return to the NM-CIDS prompt.

**Step 4** 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 5** Suspend and close the session to 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 6** Disconnect from the router:

```
router# disconnect
```

**Step 7** Press **Enter** to confirm the disconnection:

```
router# Closing connection to 10.16.0.0 [confirm] <Enter>
```

---

## Telnetting to 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 in [Configuring IDS-Sensor Interfaces on the Router, page 16-2](#).

The port number is determined by the following formula:  $2001 + 32 \times \text{slot number}$ .

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 10.16.0.0 2033
```

## 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 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 into the router and before encryption leaving the router.

---

To configure packet capture on 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's interfaces.

---

**Step 6** Configure the interface to copy network traffic to 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 through 6 for each interface or subinterface that you want to monitor.

**Step 9** Exit global configuration mode:

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

**Step 10** Verify that NM-CIDS is analyzing network traffic.

a. Open a Telnet or SSH session to the external interface on NM-CIDS.




---

**Note** SSH requires allowed hosts. For the procedure, see [Adding Hosts to the Known Hosts List, page 4-31](#).

---

b. Log in to 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 NM-CIDS is receiving network traffic.

If the counters are not increasing, make sure the you executed Steps 3 though 6 properly and that FastEthernet0/0 was added to the virtual sensor when you initialized the NM-CIDS with the **setup** command.

## Administrative Tasks for NM-CIDS

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

- [Shutting Down, Reloading, and Resetting NM-CIDS, page 16-7](#)
- [Checking the Status of the Cisco IPS Software, page 16-7](#)

### Shutting Down, Reloading, and Resetting NM-CIDS

The Cisco IOS provides the following commands to control 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 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 NM-CIDS:

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

- **reset**—Resets the hardware on 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 NM-CIDS. If 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 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 NM-CIDS.
  - **service-module ids-sensor slot\_number/0 reset**  
Provides a hardware reset to 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 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 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.