Installing the IDS Appliance

This chapter contains the following topics:

- Introducing the IDS Appliance, page 1-1
- Your Network Topology, page 1-3
- How the IDS Appliance Functions, page 1-2
- Placing an IDS Appliance on Your Network, page 1-5
- Deployment Considerations, page 1-7
- Installing the IDS Appliance, page 1-8

Introducing the IDS Appliance

The IDS appliance (models IDS-4210, IDS-4220-E, IDS-4230-FE, IDS-4235, IDS-4250-TX, IDS-4250-SX, and IDS-4250-XL) is a high-performance, plug-and-play appliance. The IDS appliance is a component of the Intrusion Detection System (IDS), a network-based, real-time intrusion detection system. You can use the Command Line Interface (CLI), IDS Device Manager, or Management Center for IDS Sensors to configure the IDS appliance. Refer to the IDS documentation on Cisco.com for more information about how to configure the IDS appliance.

You can configure the IDS appliance to respond to recognized signatures as it captures and analyzes network traffic. These responses include logging the event, forwarding the event to the IDS manager, performing a TCP reset, generating an IP log, and/or reconfiguring a router.

Note The following IDS appliance models are legacy models and are not supported in this document: NRS-2E, NRS-2E-DM, NRS-2FE, NRS-2FE-DM, NRS-TR, NRS-TR-DM, NRS-SFDDI, NRS-SFDDI-DM, NRS-DFDDI, NRS-DFDDI-DM, IDS-4220-TR, IDS-4230-SFDDI, and IDS-4230-DFDDI.

Caution Installing the latest IDS software (version 4.0) on unsupported models may yield unpredictable results. Cisco Systems does not support software installed on unsupported platforms.

After being installed at key points in the network, the IDS appliance monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, IDS appliances can terminate the specific connection, permanently block the attacking host, log the incident and send an alarm to an IDS manager. Other legitimate connections continue to operate independently without interruption.

IDS appliances can also monitor and analyze syslog messages from Cisco routers to detect and report network security policy violations.

IDS appliances are optimized for specific data rates. In switched environments, IDS appliances must be connected to the switch's Switched Port Analyzer (SPAN) port.

How the IDS Appliance Functions

The next step in protecting your network is understanding how the IDS appliance captures network traffic.

Each IDS appliance comes with two interfaces. In a typical installation, one interface monitors the desired network segment, and the other interface communicates with the IDS management workstation and other network devices. The monitoring interface is in promiscuous mode, meaning it has no IP address and is not visible on the monitored segment.

The control interface is always Ethernet. This interface has an assigned IP address, which allows it to communicate with the IDS manager workstation or network devices (typically a Cisco router). This interface is visible on the network and must be protected through SSH.

When responding to attacks, the IDS appliance can do the following:

- Insert TCP resets via the monitoring interface.

  Note The TCP reset action is only appropriate as an action selection on those signatures that are associated with a TCP-based service. If selected as an action on non-TCP-based services, no action is taken. Additionally, TCP resets are not guaranteed to tear down an offending session because of limitations in the TCP protocol.

- Make access control list (ACL) changes on routers that the IDS appliance manages.

  Note ACLs may block only future traffic, not current traffic.

- Block traffic via the control interface.

The last step in understanding how a IDS appliance functions is the data speed or load on the monitored network. Because the IDS appliance is not in the data path, it has a negligible impact on network performance. However, there are limitations on the data speeds it can monitor.

Your Network Topology

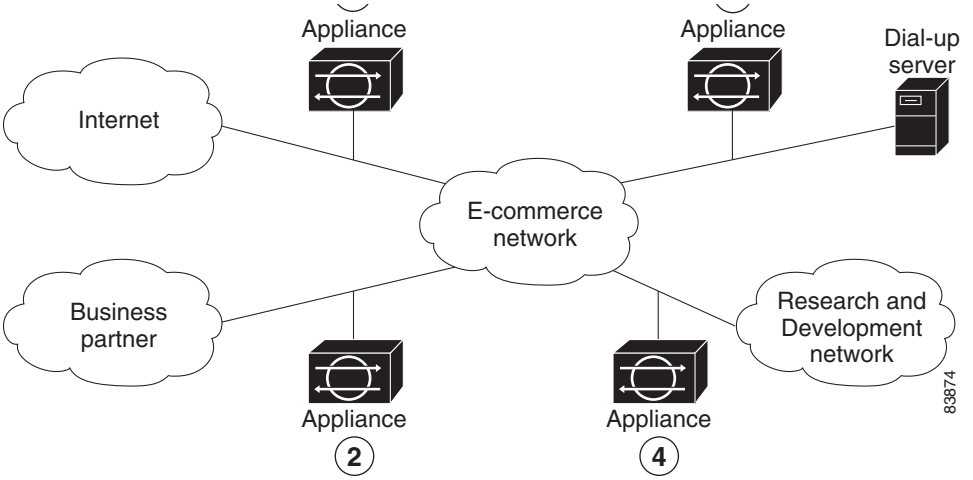
Before you deploy and configure your IDS appliances, you should understand the following about your network:

- The size and complexity of your network.
- Connections between your network and other networks (and the Internet).
- The amount and type of network traffic on your network.

This knowledge will help you determine how many IDS appliances are required, the hardware configuration for each IDS appliance (for example, the size and type of network interface cards), and how many IDS management workstations are needed.

The IDS appliance monitors all traffic across a given network segment. With that in mind, you should consider all the connections to the network you want to protect. These connections fall into four basic categories, or locations, as illustrated in Figure 1-1.

Figure 1-1 Major Types of Network Connections



In location one, the IDS appliance is placed to monitor traffic between the protected network and the Internet. This is referred to as perimeter protection and is the most common deployment for a IDS appliance. This location can be shared with firewall protection and is discussed in Placing an IDS Appliance on Your Network, page 1-5.

In location two, the IDS appliance is monitoring an extranet connection with a business partner. Although most companies have defined policies on the use and security of this type of connection, there is no guarantee that the network of a partner is adequately protected. Consequently, an outsider may enter your network through this type of connection. These extranet connections may have firewalls as well.

In location three, the IDS appliance is monitoring the network side of a remote access server. Although this connection may be only for employee use, it could be vulnerable to external attack.

In location four, the IDS appliance is monitoring an intranet connection. For example, the protected network of one department may contain an e-commerce site where all the access types described so far are required. The network of another department may contain company-specific research and development or other engineering information and should be given additional protection.

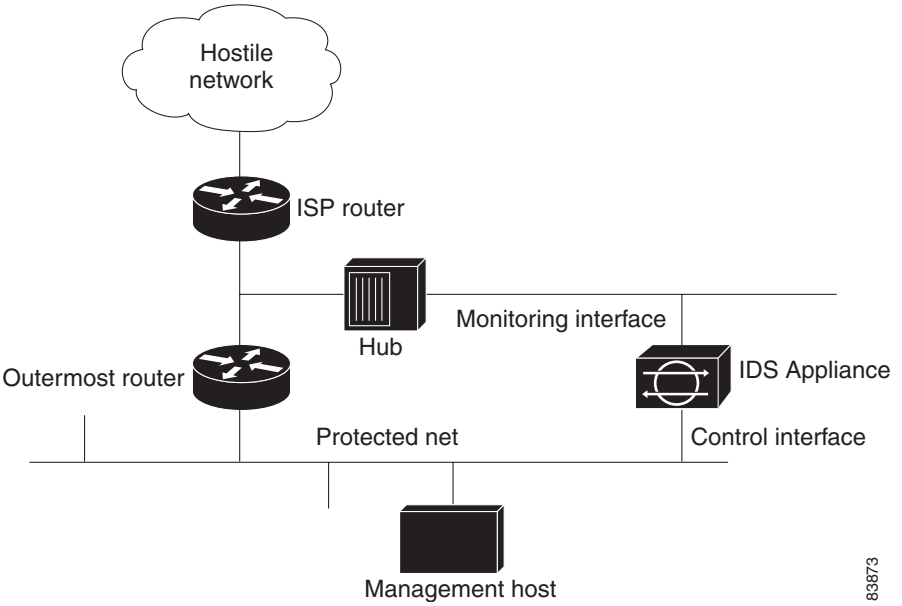
Determine the type of location you have to determine which segments of the network you want to monitor. Keep in mind that each IDS appliance maintains a security policy configured for the segment it is monitoring. The security policies can be standard across the organization or unique for each IDS appliance. You may consider changing your network topology to force traffic across a given monitored network segment. There are always operational trade-offs when going through this process. The end result should be a rough idea of the number of IDS appliances required to protect the desired network.

Placing an IDS Appliance on Your Network

You can place an IDS appliance in front of or behind a firewall. Each position has its benefits and drawbacks.

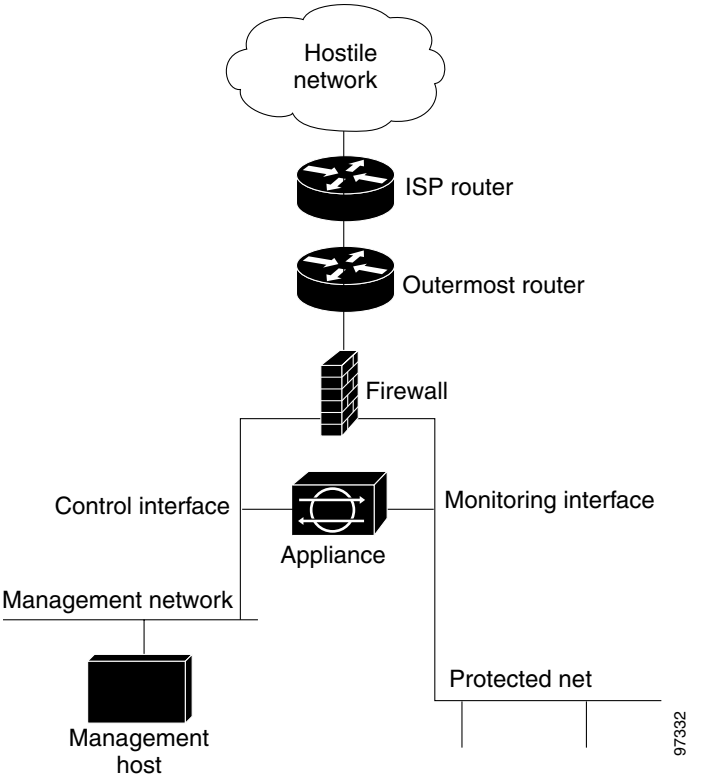
Placing an IDS appliance in front of a firewall allows the IDS appliance to monitor all incoming and outgoing network traffic. However, when deployed in this manner, the IDS appliance does not normally detect traffic that is internal to the network. An internal attacker taking advantage of vulnerabilities in network services would remain undetected by the external IDS appliance (see Figure 1-2).

Figure 1-2 IDS Appliance in Front of a Firewall



Placing an IDS appliance (a monitoring or sniffing interface) behind a firewall shields the IDS appliance from any policy violations that the firewall rejects (see Figure 1-3).

Figure 1-3 IDS Appliance Behind a Firewall



Deployment Considerations

For the IDS appliance to effectively defend a network with a router and firewall configuration, you must do the following:

- Enable Telnet services on the router.
- Add the router to the device management list of the IDS appliance (via the IDS manager).

- Configure the firewall to permit the following traffic:
  - Telnet traffic from the control interface of the IDS appliance to the router.
  - Syslog (UDP port 514) traffic from the router to the IDS appliance.

    Note To capture policy violations on the router, the IDS appliance must also be configured to accept syslog messages.

  - Communications (UDP port 45000) between the IDS appliance and any IDS manager workstation, if the firewall comes between them.

  Essentially, the firewall implements policy filtering. The IDS appliance captures packets between the Cisco router and the firewall, and can dynamically update the ACLs of the Cisco router to deny unauthorized activity.

Installing the IDS Appliance

This section contains the following topics:

- Recommended Keyboards and Monitors, page 1-9
- Installing Spare Hard-Disk Drives in the IDS-4235 and IDS-4250, page 1-9
- IDS Appliance Restrictions, page 1-10
- Upgrading the BIOS on the IDS-4235 and IDS-4250, page 1-10
- Upgrading the IDS-4220-E and IDS-4230-FE to Version 4.0, page 1-11
- Upgrading the IDS Appliance to Version 4.0, page 1-12
- Installing the IDS Appliance, page 1-19

Recommended Keyboards and Monitors

Some keyboards and monitors are not compatible with the IDS appliance. This incompatibility could cause the IDS appliance not to boot properly. We recommend that you use the following keyboards and monitors with the IDS appliance:

- Keyboards
  - KeyTronic E03601QUS201-C
  - KeyTronic LT DESIGNER
- Monitors
  - MaxTech XT-7800
  - Dell D1025HT

Caution The IDS appliance does not function properly with some HP keyboards and with IBM model G50 monitors.

Installing Spare Hard-Disk Drives in the IDS-4235 and IDS-4250

Do not install a second hard-disk drive in the 4235 and 4250 appliances. The spare hard-disk drives are meant to be replacements for the original hard-disk drives and are not meant to be used with the original hard-disk drive. If you install two hard-disk drives in the appliance, the appliance may not to be able to recognize the **recover** command used to re-image the appliance.

If the original hard-disk drive becomes unusable, remove the hard-disk drive and insert the replacement hard-disk drive. To install the version 4.0 software, use the procedure described in Upgrading the IDS Appliance to Version 4.0, page 1-12, beginning with Step 3.

IDS Appliance Restrictions

The following restrictions apply to the use and operation of the IDS appliance:

- The IDS appliance is not a general purpose workstation.
- Cisco Systems prohibits using the IDS appliance for anything other than operating Cisco IDS.
- Cisco Systems prohibits modifying or installing any hardware or software in the IDS appliance that is not part of the normal operation of the Cisco IDS.

Upgrading the BIOS on the IDS-4235 and IDS-4250

You must upgrade the BIOS on your IDS-4235 and IDS-4250 appliances before you install the version 4.0 software.

Warning **Do not apply this BIOS upgrade to appliance models other than the IDS-4235 and IDS-4250.**

To create and boot the IDS-4235 or IDS-4250 BIOS upgrade diskette, follow these steps:

Step 1 Copy BIOS_A04.exe to a Windows system.

You can find the file in the /BIOS directory on the Cisco Intrusion Detection System 4.0 Upgrade/Recovery CD, or you can download it from Cisco.com. Refer to *Release Notes for the Cisco Intrusion Detection System Version 4.0* for the procedure for getting to the IDS version 4.0 page on Cisco.com.

Note You must have a Cisco.com account with cryptographic access before you can download software from the IDS page. Refer to *Release Notes for the Cisco Intrusion Detection System Version 4.0* for the procedure.

Step 2 Insert a blank 1.44-MB diskette in the Windows system.

Step 3 Double-click the downloaded BIOS update file, BIOS_A04.exe, on the Windows system to generate the BIOS update diskette.

Step 4 Insert the newly created BIOS update diskette in your IDS-4235 or IDS-4250.

Warning **Do not power off or manually reboot the appliance during Step 5.**

Warning **You cannot upgrade the BIOS from a console connection. You must connect a keyboard and monitor to the appliance so that you can see the output on the monitor.**

Step 5 Boot the IDS appliance and follow the on-screen instructions.

Step 6 Remove the BIOS update diskette from the appliance while the appliance is rebooting, otherwise the BIOS upgrade will be started again.

Upgrading the IDS-4220-E and IDS-4230-FE to Version 4.0

If you are upgrading an IDS-4220-E or IDS-4230-FE appliance, you must swap the command and control interface cable with the sniffing interface cable before you upgrade the software. For IDS software version 4.0, the former command and control interface is now the sniffing interface.

Warning **If the cables on the IDS-4220-E or IDS-4230-FE are not swapped, you may not be able to connect to your appliance through the network.**

Note The PCI-based card that was used as the sniffing interface for the IDS-4220-E and the IDS-4230-FE does not support the monitoring of dot1q trunk packets and the tracking of the 993 Dropped Packet alarm. The performance is also lower with the PCI-based card compared to the onboard NIC. For these reasons, the PCI card is now used as the command and control interface and the onboard NIC is used for sniffing.

See Upgrading the IDS Appliance to Version 4.0, page 1-12, for the procedure.

Upgrading the IDS Appliance to Version 4.0

To upgrade your IDS appliance from IDS software version 3.1 to version 4.0, you must install the new 4.0 image from the 4.0 CD. You will need your configuration information to initialize your appliance with the 4.0 software. You can obtain this information by generating a diagnostics report through the IDS Device Manager.

Signature updates, which include the Network Security Database (NSDB), occur every two weeks. You may not have the latest signature update on the 4.0 CD. To ensure that you have the latest signatures, refer to *Release Notes for the Cisco Intrusion Detection System Version 4.0* for the procedure for obtaining the latest version 4.0 updates.

To upgrade from version 3.1 to 4.0, follow these steps:

Step 1 Obtain your appliance configuration information from the IDS Device Manager:

a. Select **Administration > Diagnostics**.

   The Diagnostics panel appears.

b. Click **Run Diagnostics**.

   Note Running the diagnostics may take a while.

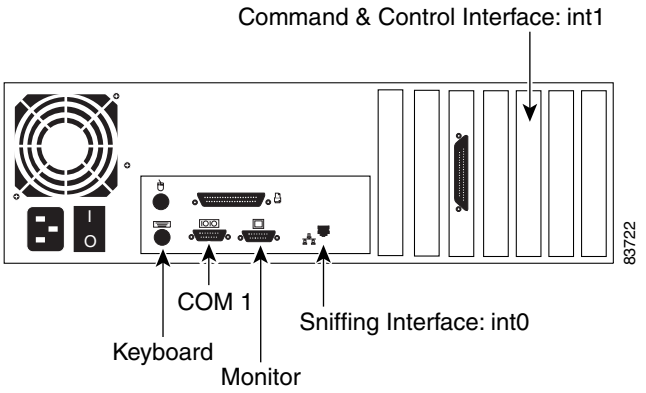
c. Click **View Results**.

   Result: The results are displayed in a report.

d. To save the diagnostics report, select **Menu > Save As** in your browser.

Step 2 If you have an IDS-4220-E or an IDS-4230-FE, swap the command and control interface cable with the sniffing interface cable. See Figure 1-4.

Figure 1-4 IDS-4220-E and IDS-4230-FE



Step 3 Power on the appliance

Step 4 Insert the Cisco IDS 4.0(1) Upgrade/Recovery CD into the CD-ROM drive.

The following boot menu lists important notices and boot options.

```
IDS-4220/4230 customers:
Sniffing and Command-and-Control interfaces have been swapped in CIDS
4.0. Reference the 4.0 software documentation before proceeding.

IDS-4235/4250 customers:
BIOS version "A04" or later is required to run CIDS 4.0 on your
appliance. Reference the 4.0 software documentation before proceeding.

- To recover the Cisco IDS 4.0 Application using a local
keyboard/monitor, type: k <ENTER>. (WARNING: ALL DATA ON DISK 1 WILL
BE LOST)

- To recover the Cisco IDS 4.0 Application using a serial connection,
type: s <ENTER>, or just press <ENTER> (WARNING: ALL DATA ON DISK 1
WILL BE LOST)
```

Step 5 Enter **k** if you are installing from a keyboard, or enter **s** if you are installing from a serial connection.

Note A blue screen is displayed for several minutes without any status messages while the files are copied from the CD to your system.

Step 6 Log in to the IDS appliance by using a serial connection or with a monitor and keyboard.

Note The default username and password are both cisco.

Step 7 You are prompted to change the default password.

Note Passwords must be at least eight characters long and be strong, that is, not be a dictionary word.

After you change the password, the `sensor#` prompt appears.

Step 8 Enter the **setup** command.

The System Configuration Dialog is displayed

Note The System Configuration Dialog is an interactive dialog. The default settings are displayed.

Step 9 Press the spacebar to get to the following question:

```
Continue with configuration dialog? [yes]:
```

Note Press the spacebar to show one page at a time.

Step 10 Enter **yes** to continue.

Step 11 Enter the following information:

- Host name

  The host name is a case-sensitive character string up to 256 characters. Numbers, "_" and "-" are valid, but spaces are not acceptable. The default is sensor.

- IP address

  An IP address is a 32-bit address written as four octets separated by periods, X.X.X.X, where X=0-255. The default is 10.1.9.201.

- Netmask

  The netmask is a 32-bit address written as four octets separated by periods, X.X.X.X, where X=0-255. The default for a Class C address is 255.255.255.0.

- Default gateway

  The default gateway is the default router IP address for the appliance. The default is 10.1.9.1.

- Telnet server status

  You can disable or enable Telnet services. The default is disabled.

- Web server port

  The web server port is the TCP port used by the web server (1 to 65535). The default is 443.

Note If you change the web server port, you must specify the port in the URL address of your browser when you connect to IDS Device Manager, in the format `https://`*sensor ip address*`:port` (for example, `https://10.1.9.201:1040`).

Step 12 Enter **yes** to save the configuration.

```
Use this configuration? [yes]: yes
Configuration Saved.
Warning: The node must be rebooted for the changes to go into effect.
```

Step 13 Enter **no** to avoid rebooting the sensor at this time.

If you modified the IP address, netmask, default gateway or web port, you are prompted for reboot.

```
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is
rebooted. Please use the reset command to complete the configuration.
```

See Step 23 for the **reset** command.

Step 14 Modify the network access lists to allow remote access:

a. Enter configure terminal mode:

```
sensor# configure terminal
```

b. Enter host configuration mode:

```
sensor(config)# service host
```

c. Enter network parameters configuration mode:

```
sensor(config-Host)# networkParams
```

d. View the current settings:

```
sensor(config-Host-net)# show settings
networkParams
 ----------------------------
 ipAddress: 10.1.9.201
 netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.1.9.1
hostname: sensor
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 1)
----------------------------
ipAddress: 10.0.0.0
netmask: 255.0.0.0 default: 255.255.255.255
```

e. Remove the 10.0.0.0 network from the access list:

```
sensor(config-Host-net)# no accessList ipAddress 10.0.0.0 netmask
255.0.0.0
```

Note The access list contains a default network address entry 10.0.0.0/255.0.0.0. You must remove this and modify the access list to suit your network.

f. To enter single host to the access list, use the following command:

```
sensor(config-Host-net)# accessList ipAddress 10.1.2.3
```

g. To add an entire network to the access list, use the following command:

```
sensor(config-Host-net)# accessList ipAddress 10.10.10.0 netmask
255.255.255.0
```

Note Enter the netmask if the IP address is a network address (as opposed to a host address).

h. Repeat Steps f and g for each address that you want to add to the access list.

i. View your changes:

```
sensor(config-Host-net)# show settings
networkParams
---------------------------
ipAddress: 10.1.9.201
netmask: 255.255.255.0 default: 255.255.255.0
defaultGateway: 10.1.9.1
hostname: sensor
telnetOption: disabled default: disabled
accessList (min: 0, max: 512, current: 2)
---------------------------
ipAddress: 10.1.2.3
netmask: 255.255.255.255 <defaulted>
---------------------------
ipAddress: 10.10.10.0
netmask: 255.255.255.0 default: 255.255.255.255
```

j. Exit network parameters configuration mode:

```
sensor(config-Host-net)# exit
```

Step 15 Configure the time:

a. Enter time parameter configuration mode:

```
sensor(config-Host)# timeParams
```

b. Specify the standard time offset from UTC in minutes (negative numbers represent time zones west of the Prime Meridian):

```
sensor(config-Host-tim)# offset -360
```

c. Specify the standard time zone:

```
sensor(config-Host-tim)# standardTimeZoneName CST
```

d. Enter summertime parameter configuration mode:

```
sensor(config-Host-tim)# summerTimeParams
```

e. Specify that summertime parameters recur at the same time each year:

```
sensor(config-Host-tim-sum)# active-selection recurringParams
```

f. Enter recurring summertime parameter configuration mode:

```
sensor(config-Host-tim-sum)# recurringParams
```

g. Specify the summertime time zone name:

```
sensor(config-Host-tim-sum-rec)# summerTimeZoneName CDT
```

Note The default recurring summertime parameters are correct for time zones in the United States. The default values specify a start time of 2 a.m. on the first Sunday in April, and a stop time of 2 a.m. on the fourth Sunday in October. The default summertime offset is 60 minutes.

h. Exit time parameter configuration mode:

```
sensor(config-Host-tim-sum-rec)# exit
sensor(config-Host-tim-sum)# exit
sensor(config-Host-tim)# exit
```

Step 16 Exit configure host mode:

```
sensor(config-Host)# exit
```

Step 17 Enter **yes** to apply the changes.

Step 18 Enter **no** to avoid rebooting the sensor at this time.

```
Warning: The node must be rebooted for the changes to go into effect.
Continue with reboot? [yes]: no
Warning: The changes will not go into effect until the node is
rebooted. Please use the reset command to complete the configuration.
```

See Step 23 for the **reset** command.

Step 19 Exit configure terminal mode:

```
sensor(config)# exit
```

Step 20 Set the clock:

clock set *hh:mm month day year*

Step 21 Generate the self-signed X.509 certificate (needed by TLS) by entering the following command:

```
sensor# tls generate-key
MD5 fingerprint is 47:B4:C9:36:B1:E7:D2:5E:D1:3E:F6:B7:83:F4:68:60
SHA1 fingerprint is
8B:26:BB:EB:04:D4:9F:27:02:0E:25:F7:BE:0E:91:4F:B8:0A:CF:7B
```

Step 22 Write down the certificate fingerprints.

You will need these to check the authenticity of the certificate when connecting to this sensor with a web browser.

Step 23 Reboot the sensor:

```
sensor# reset
```

Step 24 Enter **yes** to continue rebooting the sensor.

```
Warning: Executing this command will stop all applications and reboot
the node.
Continue with reset? : yes
Request Succeeded.
```

Installing the IDS Appliance

To install the IDS appliance, follow these steps:

Step 1 Position the IDS appliance on the network.

See Placing an IDS Appliance on Your Network, page 1-5, for information on the best places to position a IDS appliance.

Step 2 Attach the power cord to the IDS appliance and plug it into a power source (a UPS is recommended).

Note When you first plug an IDS-4210 in to a power source, it powers on momentarily and then powers off leaving the Network Interface Card (NIC) link lights lit. This is normal behavior. Press the power switch to boot the system into operation.

Step 3 Use the dual serial communication cable (PN 72-1847-01, included in the accessory kit) to attach a laptop to the COM1 port of the IDS appliance (see Table 1-1 for a list of the terminal settings), or connect a keyboard and monitor to the IDS appliance.

Table 1-1 Terminal Settings

Terminal	Setting
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	Hardware or RTS/CTS

Caution We recommend that you use the dual serial communication cable (PN 72-1847-01, included in the accessory kit) rather than a keyboard and monitor, because some keyboards and monitors are incompatible with the IDS appliance. See Recommended Keyboards and Monitors, page 1-9, for a list of compatible monitors and keyboards.

Step 4 Identify the type of IDS appliance you have by comparing its back panel to Figure 1-5, Figure 1-6, or Figure 1-7.

Caution If you are upgrading an IDS-4220-E or IDS-4230-FE, you must swap the network cables. The former command and control interface is now the sniffing interface. See Upgrading the IDS-4220-E and IDS-4230-FE to Version 4.0, page 1-11, for more information.

Warning **If the cables on the IDS-4220-E or IDS-4230-FE are not swapped, you may not be able to connect to your appliance through the network.**

Step 5 Attach the network cables accordingly.

Figure 1-5 IDS-4220-E and IDS-4230-FE

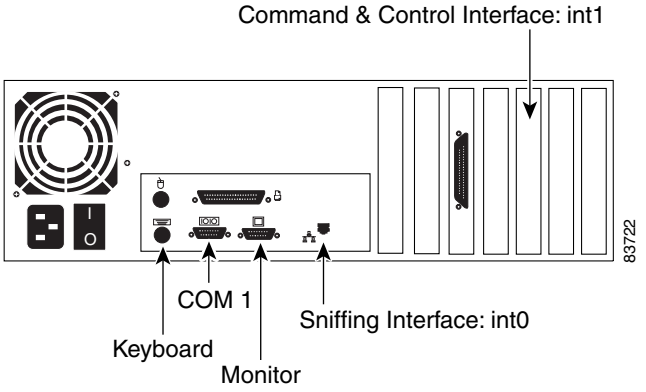


Figure 1-6 IDS-4210

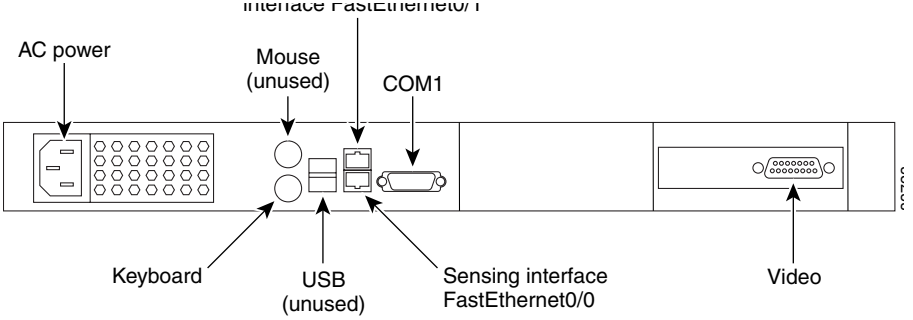
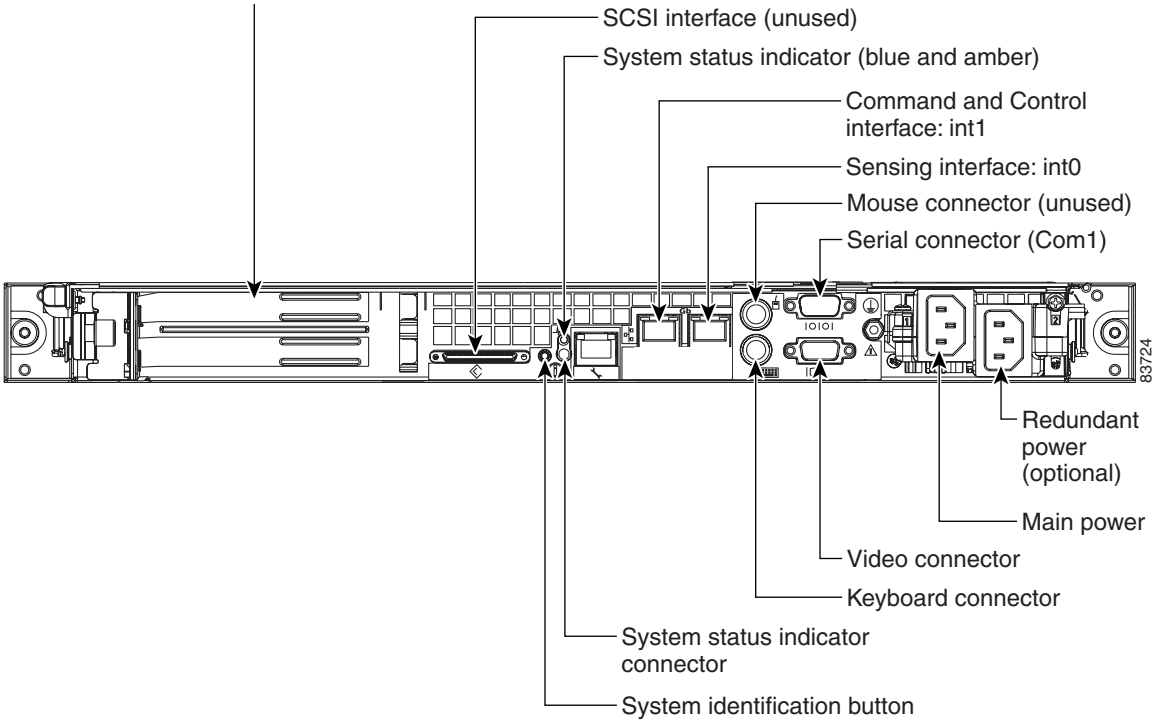


Figure 1-7 IDS-4235, IDS-4250-SX, and IDS-4250-TX



Step 6 Power on the IDS appliance.

Note If you have an IDS-4235 or IDS-4250, you must apply the BIOS upgrade before installing the version 4.0 software. See Upgrading the BIOS on the IDS-4235 and IDS-4250, page 1-10.

You are now ready to configure your IDS appliance. See Initializing the Sensor, page 4-7, for the procedure for initializing the sensor.