
# Nortel TPS 3D Sensor and Defense Center Installation Guide

**TPS 3D Sensors 2050, TPS 2150, TPS 2070, TPS 2170, and Defense Center TPS 2070 DC**

**Santa Clara, California 95054**
**USA**

**Release 4.7.0**

Part No. NN47240-300
(320737-B)

840712030644

# TABLE OF CONTENTS

# CHAPTER 1
# BEFORE YOU BEGIN

***IMPORTANT!*** Beginning with Release 4.7 software, 3D Sensors refer to both Intrusion Sensors and RTI Sensors. A 3D Sensor is able to have Intrusion Sensing (IPS/IDS) and/or RTI capabilities.

This guide describes how to install and set up the Nortel 3D Sensor. Depending on which Nortel 3D System products you have licensed, a Nortel 3D Sensor can include:

- IPS, the intrusion detection and prevention component
- RNA, the Real-time Network Awareness component
- RUA, the Real-time User Awareness component
- any two components, or all three

Each of the components is described in detail in the Nortel TPS 3D System User Guide. You can install a 3D Sensor with the IPS component as a standalone appliance, but if you want to use RNA or RUA, you must use the 3D Sensor with a Defense Center. Note that some models of the 3D Sensor do not support every combination of components. See “Understanding detection engines and interface sets” on page 18 for more information.

Before you install a Nortel 3D Sensor, you should consider how your network is configured and how you want to deploy the various components of the Nortel TPS 3D System within it.

This chapter describes some of the considerations for deploying a 3D Sensor, including:

- the concept of the detection engine and the modes in which you can deploy detection engines on the 3D Sensor: passive or inline
- your goals in deploying sensors that use RNA to perform network discovery and vulnerability assessment, as well as your goals in deploying sensors

- that use IPS to detect and prevent attacks on your network assets deployment issues, such as which network segments you want to monitor with your 3D Sensors, and why
- how you will physically connect the sensors to your network, taking into account any special network configuration factors, such as firewall placement, VPN deployments
- whether you will use a Nortel Defense Center to aggregate and correlate RNA and intrusion events

See the following sections for more information.


- "IPS installation considerations" on page 6
- "RNA installation considerations" on page 7"
- "RUA installation considerations" on page 7
- "Typical 3D Sensor deployments" on page 8
- "Other deployment options" on page 15
- "Understanding detection engines and interface sets" on page 18
- "Connecting sensors to your network" on page 20
- "Using a Nortel Defense Center" on page 23


## IPS installation considerations

IPS is the intrusion prevention and detection component of the Nortel TPS 3D System. Before you install a 3D Sensor with IPS, you should consider how your network is configured and how you want to deploy the various components of the Nortel TPS 3D System within it.

Every network architecture is different, and every enterprise has different security needs. This section lists some of the factors you should consider as you formulate your deployment plans and includes a description of how the Nortel TPS 3D System can help you meet common network security goals.

Your deployment decisions for 3D Sensors with IPS will be based on a variety of factors. Answering these questions can help you understand the vulnerable areas of your network and clarify your intrusion detection and prevention needs.

- Will you be deploying your 3D Sensor with passive or inline interface sets? Does your 3D Sensor support multiple detection engines with a mix of interface sets, some passive and others inline? See "Understanding detection engines and interface sets" on page 18 for more information about detection engines and interface sets and how they influence your sensor deployment.
- How will you connect the 3D Sensors to the network? Hubs? Taps? Spanning ports on switches? See "Connecting sensors to your network" on page 20 for more information about methods for connecting the sensing interfaces on your sensor to your network.

- Do you want to detect every attack on your network, or do you only want to know about attacks that penetrate your firewall? Do you have specific assets on your network such as financial, accounting, or personnel records, production code, or other sensitive, protected information that requires special security policies? See “Typical 3D Sensor deployments” on page 8 for more information.
- Do you provide VPN or modem access for remote workers? Do you have remote offices that also require an IPS deployment? Do you employ contractors or other temporary employees? Are they restricted to specific network segments? Do you integrate your network with the networks of other organizations such as customers, suppliers, or business partners? See “Other deployment options” on page 15 for more information.

## RNA installation considerations

RNA is the Real-time Network Awareness component of the Nortel 3D System. Before you install a 3D Sensor with RNA, you should first consider your goals in deploying network discovery and vulnerability assessment sensors. Next, consider deployment issues, such as which network segments you want to monitor with RNA (and why), and how you will physically connect these appliances to your network. Finally, you should take into account any special network configuration factors, such as firewall placement, VPN deployments, and how you will use a Nortel Defense Center to aggregate and correlate RNA events.

Monitoring network changes with RNA can help you realize a variety of goals. Clarifying your network discovery and vulnerability assessment goals can guide your deployment choices. This section examines some general goals that can influence a deployment of 3D Sensors with RNA, such as:

- Gaining a more thorough understanding of your current network infrastructure.
- Learning when network change occurs and how it affects your network’s susceptibility to compromise.
- Using RNA data to refine your intrusion rules and firewall rules.

## RUA installation considerations

RUA is the Real-time User Awareness component of the Nortel 3D System. RUA allows your organization to correlate threat, endpoint, and network intelligence with user identity information. 3D Sensors with RUA allow you to identify the source of policy breaches, attacks, or network vulnerabilities. By linking network behavior, traffic, and events directly to individual users, RUA helps to mitigate risk, block users or user activity, and take action to protect others from disruption. These capabilities also significantly improve audit controls and enhance regulatory compliance.

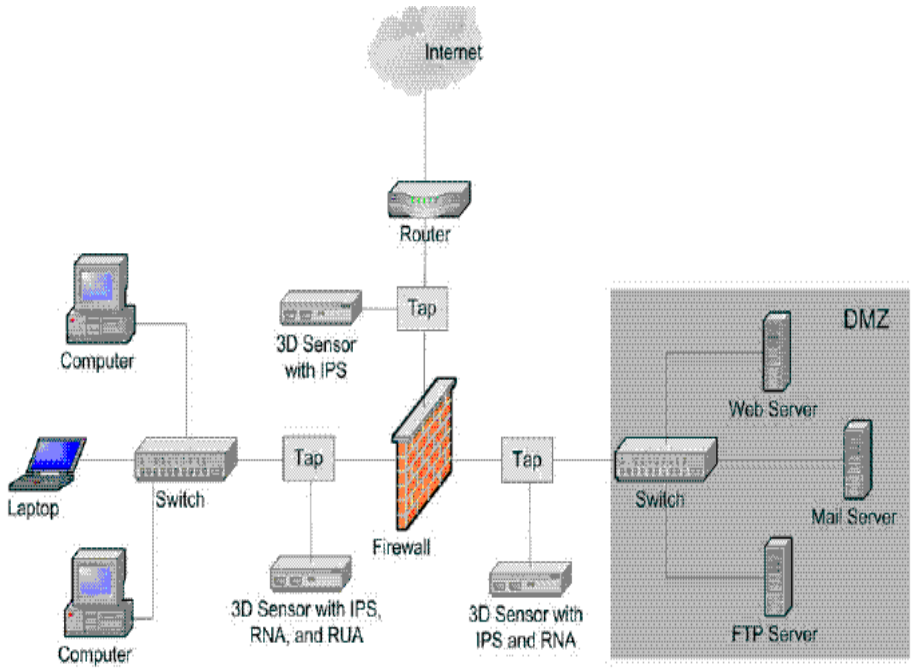
3D Sensors with RUA use detection engines to passively analyze the traffic that travels through your network. An RUA detection engine collects user login events by passively monitoring traffic. Refer to “Setting up Nortel 3D Sensors with RUA” in the Nortel TPS 3D System User Guide for more information.

## Typical 3D Sensor deployments

In the following simple network architecture diagram, the network contains three areas with three different security policies:

- between the border router and the firewall
- in the demilitarized zone, or DMZ
- in the internal, protected network

**Figure 1 Typical 3D Sensor deployments**




Deploying your 3D Sensors in each of these locations serves different purposes.

- Placement outside the firewall gives you a clear picture of all the traffic traversing your network via this gateway. Generally, this location is appropriate for IPS only. Most enterprises would not need to identify user identities or employ host and vulnerability detection capabilities in this area.
- Placement in the DMZ provides you with useful information about attacks on outward-facing servers. Generally, this location is appropriate for IPS and RNA, although some enterprises would want to add the user identification capabilities of RUA here as well.
- Placement on the internal network monitors inbound traffic for firewall misconfiguration and detects attacks that originate from hosts on the

internal network. Generally, all internal networks are ideal locations for the combined capabilities of IPS, RNA, and RUA.

---

***IMPORTANT!*** These three locations indicate where you may want to connect the 3D Sensor's sensing interfaces. Regardless of where you connect the sensing interfaces, make sure you connect the 3D Sensor's management interface to a secure internal network that is protected from unauthorized access.

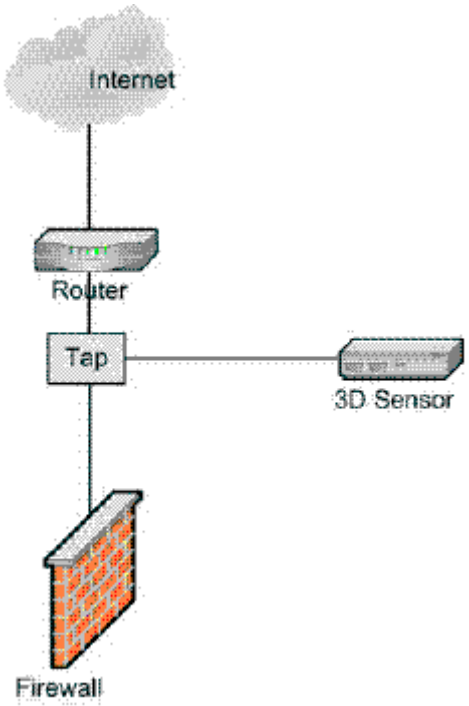
---

### Outside the firewall

Outside the firewall, the router provides the first line of defense. Although you can configure most routers to block unwanted packets, this is not typically used to secure the network segment between the router and the firewall. Placing the 3D Sensor here can help you detect attacks made against your network as well as attacks from your network to another.

Deploying the 3D Sensor on this segment of your network for a week or two can help you understand what kinds of attacks reach your firewall and where they originate. Although you can readily inspect all traffic traversing your network, considerable resources are required to prioritize, investigate, and respond to events that may be blocked by your firewall. Your enterprise's ability to gain knowledge from this approach depends on the amount of traffic traversing your network and your security analyst resources. Gaining this kind of information can help you tune your firewall rules to be as effective as possible.

**Figure 2 Outside the firewall**

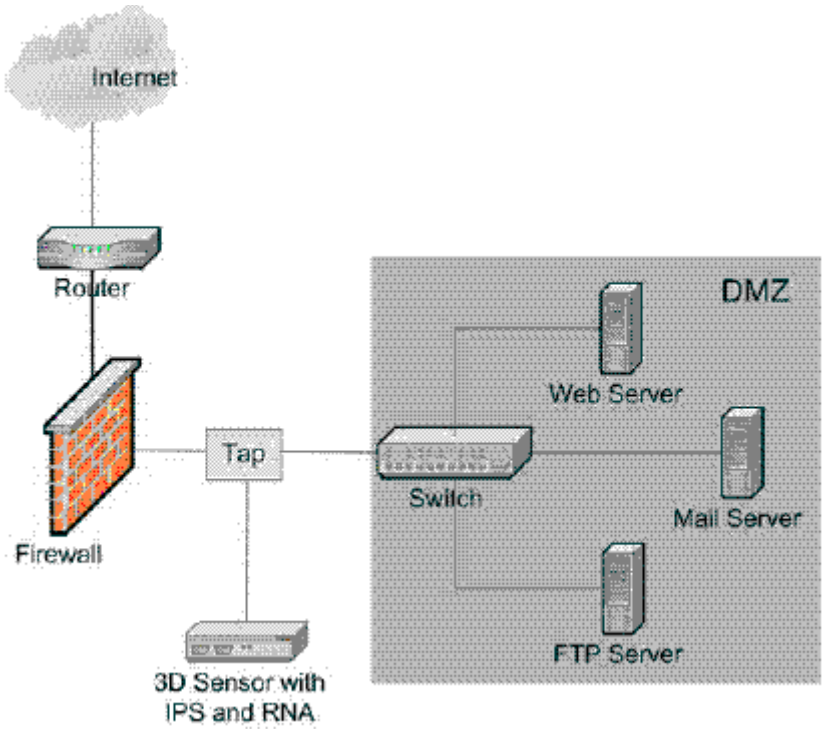



### In the DMZ

In this simple network architecture, the DMZ contains outward-facing servers (web, FTP, DNS, mail, and so on). The hosts in the DMZ provide services to external users and are at a greater security risk than those inside the firewall.

In this network configuration, the servers in the DMZ also provide services such as mail relay and web proxy to users on the internal network. A 3D Sensor with IPS on this segment can provide useful information about the kinds of attacks on outward facing servers as well as detect attacks directed to the Internet that originate from a compromised server in the DMZ. Adding RNA to the sensor on this segment can help you monitor these exposed servers for changes (for example, a new unknown service suddenly appearing) that could indicate a compromised server in the DMZ.

**Figure 3 In the DMZ**



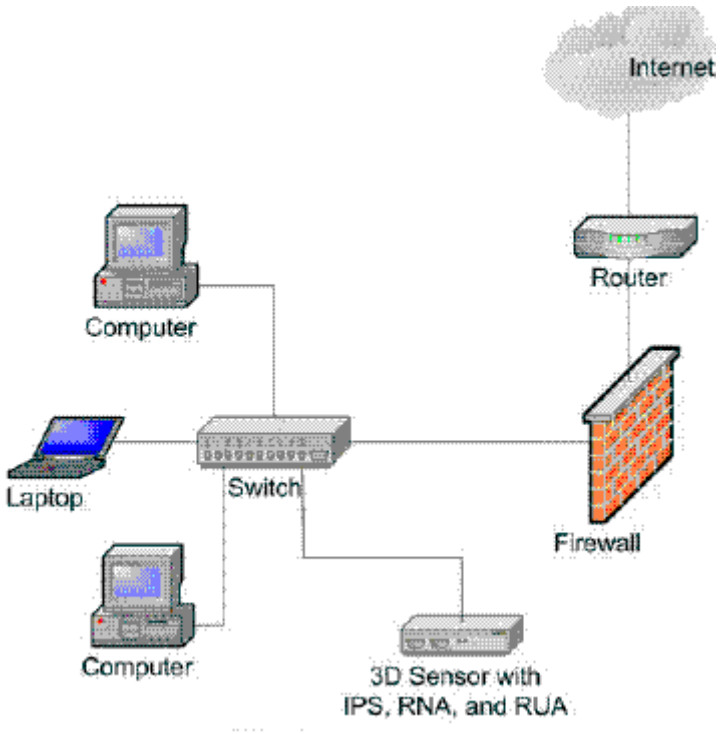

## On the internal network

Although the sample network includes a firewall configured to provide security to the servers and workstations on the internal network, 3D Sensors on this segment can monitor traffic that is allowed inbound by the firewall by choice or due to firewall misconfiguration. For example, if you have a security policy that prohibits FTP connections to any host on the internal network, you can create a rule on the 3D Sensor that will trigger when it detects traffic directed to port 21 on any IP address in the segment. A 3D Sensor on this segment can also detect attacks that originate from hosts on the internal network. For instance, attaching one 3D Sensor to a mirror or span port on a switch helps you identify attacks from one computer on the internal network directed against other computers on the internal network if the attack traffic traverses the switch.

Similarly, if a host on your network is compromised from within, RNA can immediately identify both unauthorized changes on hosts. For example, a Microsoft shop can use RNA to identify in real time a rogue Linux or Free BSD system that mysteriously appears on their network segment. RNA on a switched network segment can monitor all the hosts and services on the segment for changes and vulnerabilities. For example, attaching an 3D Sensor to a mirror or SPAN port on the switch allows you to monitor the entire network segment, as long as all traffic to and from all hosts on the segment traverses the switch.

In either case, by adding RUA to the 3D Sensor, you can immediately identify the user who is logged into the host that is running the rogue operating system or launching the internal attack.

**Figure 4 On the internal network**




## Deploying a Multi-Port 3D Sensor

Selected models of the 3D Sensor offer multiple sensing ports on an adapter card. You can use the multi-port 3D Sensors in either of two ways:

- to recombine the separate connections from a network tap
- to capture and evaluate traffic from different networks

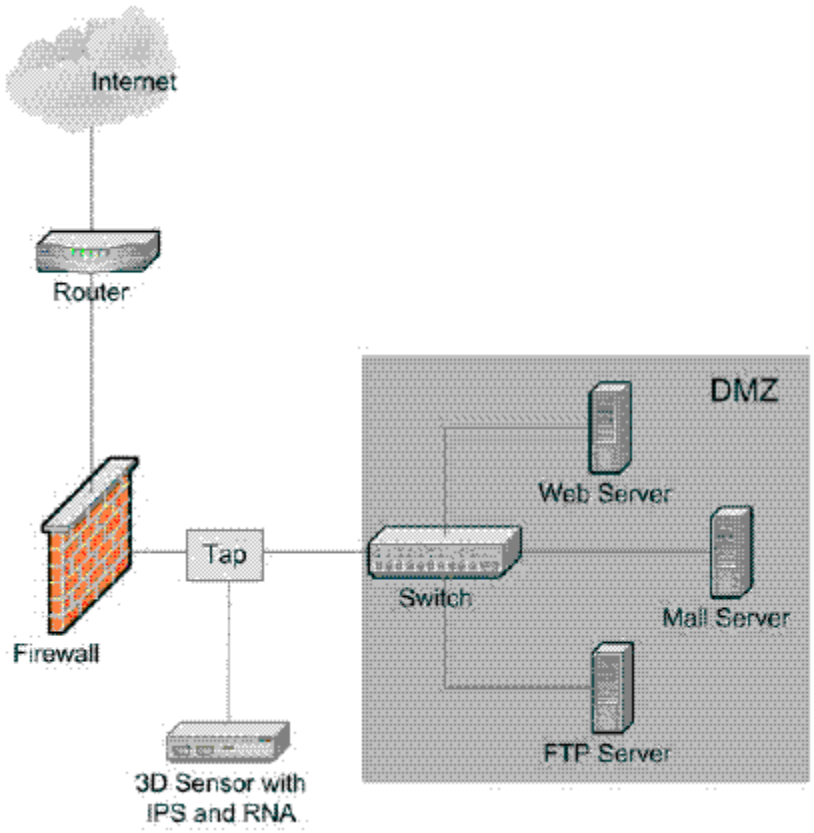
---

***IMPORTANT!*** Although each port is capable of receiving the full throughput for which the sensor is rated, the total traffic on the 3D Sensor cannot exceed its bandwidth rating without some packet loss.

---

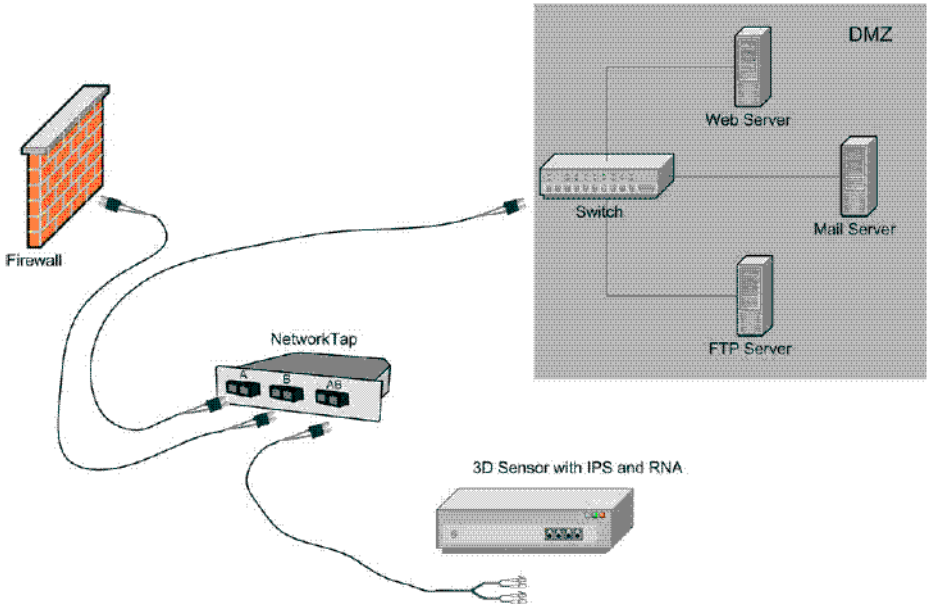
Deploying a multi-port 3D Sensor with a network tap is a straightforward process. The following illustration shows a network tap installed on a high-traffic network segment.

**Figure 5 Deploying a multi-port 3D Sensor**

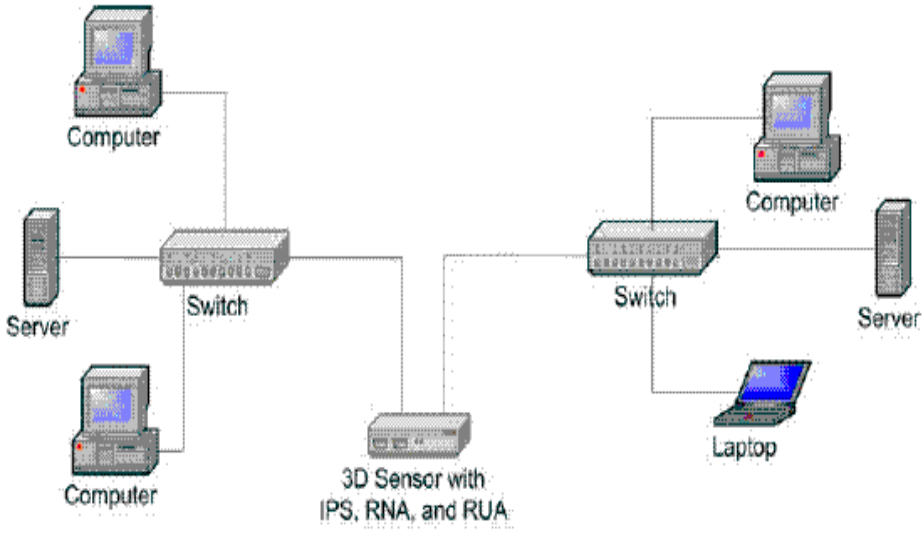



In this scenario, the tap transmits incoming and outgoing traffic through separate ports. When you connect the multi-port adapter card on the 3D Sensor to the tap, the 3D Sensor is able to combine the traffic into a single data stream so that it can be analyzed.

Note that with a gigabit optical tap, as shown in the illustration below, both sets of ports on the 3D Sensor are used by the connectors from the tap.




If your 3D Sensor supports multiple detection engines, you can also create interface sets to capture data from separate networks. The following illustration shows a single sensor with a dual-port adapter and two interface sets connected to two networks.



## Other deployment options

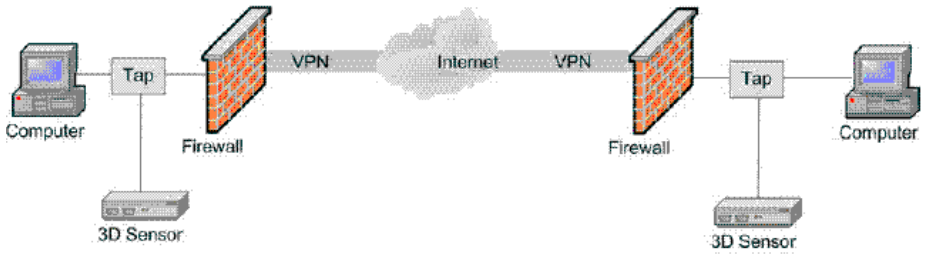
The following sections describe other installation scenarios that may affect your enterprise's deployment of the Nortel 3D System.



### Integrating with VPNs

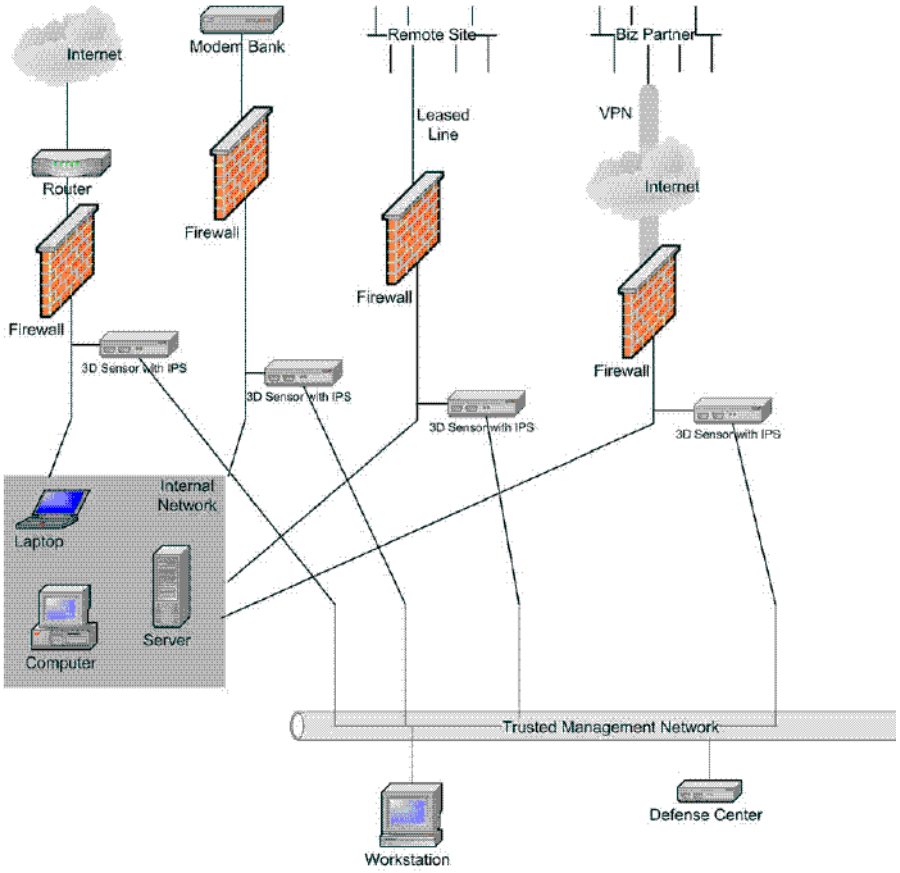
Virtual private networks, or VPNs, use IP tunneling techniques to provide the security of a local network to remote users over the Internet. In general, VPN solutions encrypt the data payload in an IP packet. The IP header is unencrypted so that the packet can be transmitted over public networks in much the same way as any other packet. When the packet arrives at its destination network, the payload is decrypted and the packet is directed to the proper host.

Because network appliances cannot analyze the encrypted payload of a VPN packet, placing 3D Sensors outside the terminating endpoints of the VPN connections ensures that all packet information can be accessed. The following diagram illustrates how 3D Sensors can be deployed in a VPN environment.



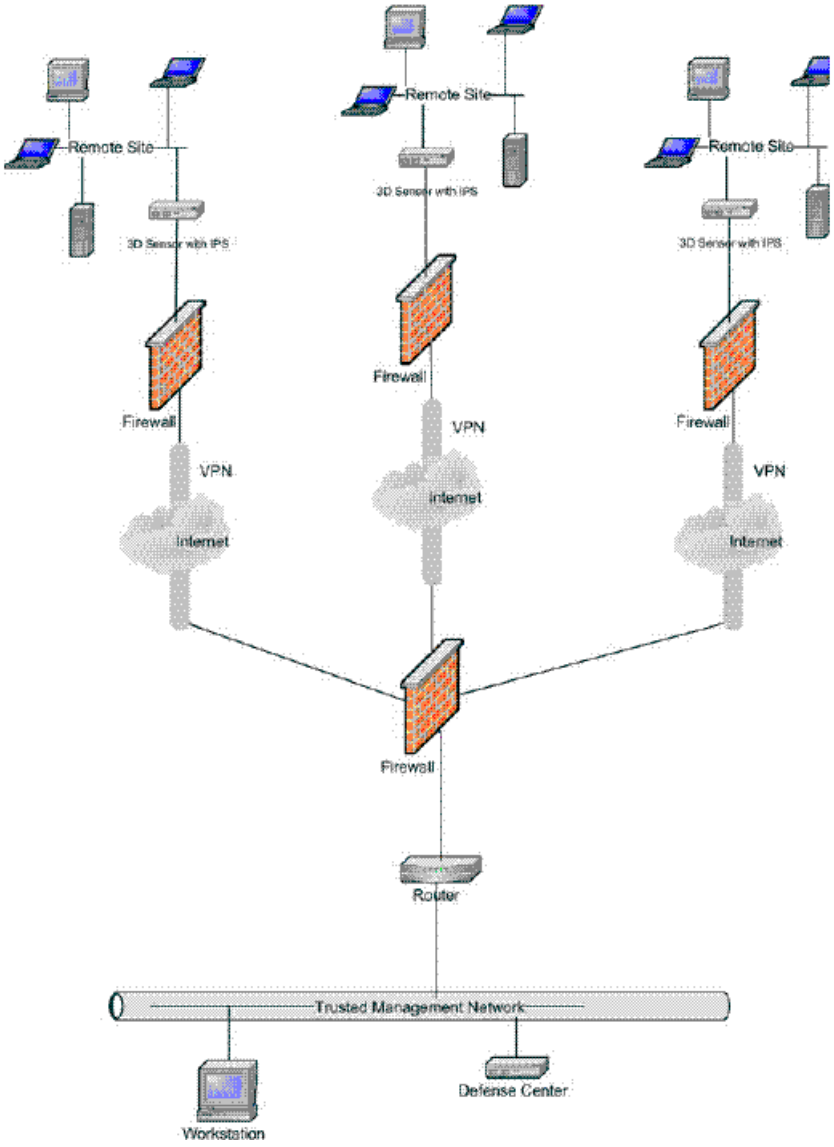

### Detecting Intrusions on other points of entry

Many networks include more than one access point. Instead of a single border router that connects to the Internet, some enterprises use a combination of the Internet, modem banks, and direct links to business partner networks. In general, you should deploy 3D Sensors near firewalls (either inside the firewall, outside the firewall, or both) and on network segments that are important to the integrity and confidentiality of your business data. The following diagram illustrates how 3D Sensors can be installed at key locations on a complex network with multiple entry points.




## Deploying in Multi-Site environments

Many organizations want to extend intrusion detection across a geographically disparate enterprise and then analyze all the IPS data from one location. The Nortel 3D System supports this by offering the Defense Center, which aggregates and correlates events from 3D Sensors deployed throughout the organization's many locations. Unlike deploying multiple 3D Sensors and Defense Centers in the same geographic location on the same network, when deploying 3D Sensors in disparate geographic locations, you must take precautions to ensure the security of the 3D Sensors and the data stream. To secure the data, you must isolate the 3D Sensors and Defense Center from unprotected networks. You can do this by transmitting the data stream from the 3D Sensors over a VPN or with some other secure tunneling protocol as shown in the following diagram.




## Integrating 3D Sensors with RNA within complex networks

You can deploy 3D Sensors with RNA in more complex network topologies than a simple multi-sector network. This section describes the issues surrounding network discovery and vulnerability analysis when deploying RNA in environments where proxy servers, NAT devices, and VPNs exist, in addition to information about using the Nortel Defense Center to manage multiple 3D Sensors and the deployment and management of 3D Sensors in a multi-site environment.

### Integrating with proxy servers and NAT

Network address translation (NAT) devices or software may be employed across a firewall, effectively hiding the IP addresses of internal hosts behind a firewall. If 3D Sensor with RNA are placed between these devices or software and the hosts being monitored, RNA may incorrectly identify the hosts behind the proxy or NAT device. In this case, Nortel recommends that you position 3D Sensors with RNA inside the network segment protected by the proxy or NAT device to ensure that hosts are correctly detected.

### Integrating with load balancing methods

In some network environments, “round robin” DNS configurations are used to perform network load balancing. In a round robin DNS system, IP addresses are shared between two or more hosts with unique operating systems. In this case, RNA will detect the operating system changes and will not be able to deliver a static operating system identification with a high confidence value. Depending on the number of different operating systems on the affected hosts, RNA may generate a large number of operating system change events or present a static operating system identification with a lower confidence value.

### Other RNA detection considerations

If an alteration has been made to the TCP/IP stack of the host being identified, RNA may not be able to accurately identify the host operating system. In some cases, this is done to improve performance. For instance, administrators of Windows hosts running the Internet Information Services (IIS) Web Server are encouraged to increase the TCP window size to allow larger amounts of data to be received, thereby improving performance. In other instances, TCP/IP stack alteration may be used to obfuscate the true operating system to preclude accurate identification and avoid targeted attacks. The likely scenario that this intends to address is where an attacker conducts a reconnaissance scan of a network to identify hosts with a given operating system followed by a targeted attack of those hosts with an exploit specific to that operating system.

## Understanding detection engines and interface sets

A detection engine is the mechanism on a 3D Sensor that is responsible for analyzing the traffic on the network segment where the sensor is connected. Depending on which components are licensed on the sensor, 3D Sensors can support three types of detection engines: IPS, RNA, and RUA.

A detection engine has two main components:

- an interface set, which can include one or more sensing interfaces
- a detection resource, which is a portion of the sensor’s computing resources

Depending on the model, some 3D Sensor with IPS can use multiple detection resources per detection engine, which allows you to use more computing resources when network traffic is high.

The number of detection engines per sensor is limited by the number of detection resources that are available. Most 3D Sensor models have at least three detection resources available and can support at least three detection engines: one for IPS, one for RNA, and the third for RUA.

RNA and RUA detection engines are limited to single detection resources per detection engine.

An interface set refers to a grouping of one or more sensing interfaces on a sensor, although a sensing interface can belong to only one interface set at a time. The Nortel 3D System supports three types of interface sets, but the interface options available to you depend on the type of sensor and the capabilities of its sensing interfaces.

**Interface Set Types**

| Type | Description |
|---|---|
| Passive | Use a passive interface set if you deployed the sensor out of band from the flow of network traffic. |
| Inline | Use an inline interface set if you deployed the sensor inline on your network and the sensing interfaces do **not** support automatic fail-open capabilities. Note that you can use any two of the non-fail-open interfaces on the sensor's network interface cards as part of an inline interface set. |
| Inline with Fail Open | Use an inline with fail open interface set if you deployed the sensor inline on your network and the sensing interfaces **do** support automatic fail-open capabilities. Note that you must use paired fail-open interfaces on the sensor's network interface cards for an inline with fail open interface set. |

The traditional scenario for deploying 3D Sensors across your network infrastructure calls for installing a different sensor in each location where you want to enforce a security policy. In other words, you may want to install one 3D Sensor in the DMZ and others on each internal network segment. If you have a network segment with hosts that are likely to be targets of specialized attacks (for example, a web host farm), you would deploy another 3D Sensor there.

Multiple IPS detection engines on a single 3D Sensor can provide you with more flexibility in deploying 3D Sensors throughout your network. A detection engine is like a virtual sensor within a sensor. When you create a detection engine on a 3D Sensor, you specify which of the sensor's sensing interfaces it uses and what portion of the sensor's detection resources it can use. You can then create and apply an intrusion policy that is tuned especially for the network attacks that are likely to be seen on the segment of the network that the detection engine monitors. See the *"Using Detection Engines and Interface Sets"* chapter in the *Nortel TPS 3D System User Guide* for more information about creating and using detection engines.

### Comparing inline and passive interface sets

An interface set is comprised of one or more sensing interfaces on the 3D Sensor. Each detection engine is assigned to an interface set and uses those interfaces to monitor the traffic on specific network segments. Interface sets can be one of the following types:

- passive
- inline
- inline with fail open

If you create an IPS detection engine that uses either type of the inline interface set, then you can deploy your detection engine inline. This allows you to create take advantage of drop rules that prevent suspicious traffic from reaching potentially vulnerable host. You can also use replace rules that substitute malicious content with a benign alternative. You can also create RNA and RUA detection engines for inline or inline with fail open interface sets.

A detection engine that uses an inline with fail open interface set has the same properties as an inline interface set with one exception. You can only use an inline with fail open interface set with fail-open network interface cards. If a 3D Sensor with a fail-open card should fail for some reason (power failure, hard drive failure, and so on), traffic is not blocked by the sensor and your network continues to function.

## Connecting sensors to your network

There are several ways to connect 3D Sensors to your network. The following sections outline the supported connection methods.

- “Using a Hub” on page 20
- “Using a span port” on page 21
- “Using a network tap” on page 21

Additionally, “Issues for Copper Cabling” on page 27 explains some of the guidelines for using straight-through or crossover cables in your deployment.

### Using a Hub

An Ethernet hub is an inexpensive way to ensure that the detection engine on a 3D Sensor can see all the traffic on a network segment. Most hubs of this type take the IP traffic meant for any of the hosts on the segment and broadcast it to all the devices connected to the hub. Connect the interface set to the hub to monitor all incoming and outgoing traffic on the segment. Using a hub does not guarantee

that the detection engine sees every packet on a higher volume network because of the potential of packet collision. For a simple network with low traffic, this is not likely to be a problem. In a high-traffic network, a different option may provide better results.

---

***IMPORTANT!*** Some devices are marketed as hubs but actually function as switches and do not broadcast each packet to every port. If you attach your 3D Sensor to a hub, but do not see all the traffic, you may need to purchase a different hub or use a switch with a Span port.

---

### Using a span port

Many network switches include a span port that mirrors traffic from one or more ports. By connecting an interface set to the span port, you can monitor the combined traffic from all ports, generally both incoming and outgoing. If you already have a switch that includes this feature on your network, in the proper location, then you can deploy the detection on multiple segments with little extra equipment cost beyond the cost of the 3D Sensor. In high-traffic networks, this solution has its limitations. If the span port can handle 200 Mbps and each of three mirrored ports can handle up to 100 Mbps, then the span port is likely to become oversubscribed and drop packets, lowering the effectiveness of the 3D Sensor.

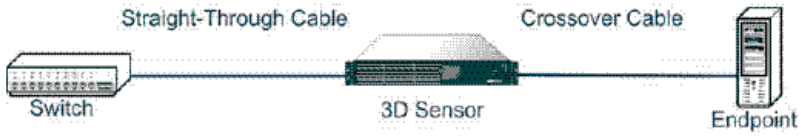
### Using a network tap

Network taps allow you to passively monitor traffic without interrupting the network flow or changing the network topology. Taps are readily available for different bandwidths and allow you to analyze both incoming and outgoing packets on a network segment. Unfortunately, you can only monitor a single network segment with most taps, so they are not a good solution if you want to monitor, for example, the traffic on two out of the eight ports on a switch. Instead, you would have to install the tap between the router and the switch and access the full IP stream to the switch.

By design, network taps divide incoming and outgoing traffic into two different streams over two different cables. Most models of the 3D Sensors offer multi-port options that recombine the two sides of the conversation so that the entire traffic stream is evaluated by the decoders, the preprocessors, and the detection engine.

### Between a Switch and an Endpoint

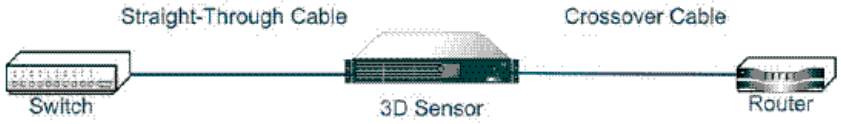
When you deploy an inline 3D Sensor between a switch and an endpoint, use a straight-through cable between the switch and the sensor and a crossover cable between the sensor and the endpoint.




When the sensor switches to bypass mode, the internal crossover and the crossover cable between the endpoint and the sensor combine to create a straight-through cable, allowing normal operation of the connection.

### Between a Router and a Switch

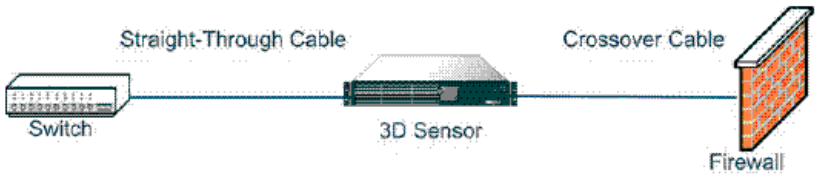
When you deploy an inline 3D Sensor between a router and a switch, use a straight-through cable between the switch and the sensor and a crossover cable between the sensor and the router.




When the sensor switches to bypass mode, the internal crossover and the crossover cable between the router and the sensor combine to create a straight-through cable, allowing normal operation of the connection.

### Between a Switch and a Firewall

When you deploy an inline 3D Sensor between a switch and a firewall, use a straight-through cable between the switch and the sensor and a crossover cable between the sensor and the firewall.




When the sensor switches to bypass mode, the internal crossover and the crossover cable between the firewall and the sensor combine to create a straight-through cable, allowing normal operation of the connection.

## Using a Nortel Defense Center

In addition to running 3D Sensors with IPS as standalone appliances, you can manage 3D Sensors with the Nortel Defense Center. The Defense Center aggregates and correlates events generated by multiple 3D Sensors on different segments of your network. You can also use the Defense Center to manage, change, and standardize the intrusion policies on 3D Sensors.

To safeguard the Defense Center, it must be installed on a protected internal network. Although the Defense Center is configured to have only the necessary services and ports available, you must make sure that attacks cannot reach it from outside the firewall.

If the 3D Sensor and the Defense Center reside on the same network, you can connect the management interface on the 3D Sensor to the same protected internal network as the Defense Center. This allows you to securely control the sensor from the Defense Center and aggregate the event data generated on the 3D Sensor's network segment. By using the Defense Center's filtering capabilities, you can analyze and correlate data from attacks across your network to evaluate how well your security policies are being implemented.

# CHAPTER 2
# INSTALLATION

This chapter describes the installation requirements for the following TPS appliances:

- TPS 3D Sensor 2050
- TPS 3D Sensor 2070
- TPS 3D Sensor 2150
- TPS 3D Sensor 2170
- TPS 2070 DC

# TPS 2070 DC

The Defense Center is an easily installed appliance designed to aggregate and communicate information received from all 3D Sensors running IPS, RNA, RUA, or a combination of the three, giving you a clear picture of your network traffic and any attacks against your network. Note that you cannot run RUA by itself on a 3D Sensor; you must combine it with either IPS, RNA, or both.

See the following sections for more information about installing a Defense Center.


- "Security considerations" on page 25
- "Installing the Defense Center DC 2070" on page 25
- "Setting the IP Address for the Management interface" on page 26
- "Performing the initial setup" on page 27
- "Console output" on page 32


## Security considerations

Before you install your Defense Center, Nortel recommends that you consider the following.

- Locate your Defense Center in a lockable rack within a secure location that prevents access by unauthorized personnel. If you are installing a desktop model, make sure you place it within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the Defense Center.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access.

## Installing the Defense Center DC 2070

To install the TPS 2070 DC, do the following:

The Defense Center is delivered on different hardware appliances. Make sure you refer to the correct illustration for your appliance as you follow the installation procedure.

To install the appliance:

1. Mount the Defense Center in your rack using the enclosed mounting kit, which has its own set of instructions.
2. Attach the power cord to the Defense Center and plug it in to a power source.

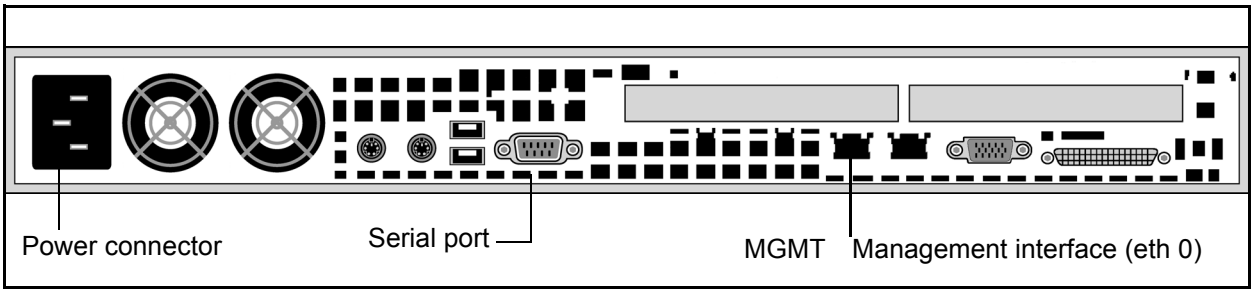
---

***IMPORTANT!*** If your Defense Center has redundant power supplies, attach power cords to both power supplies and plug them in.

---

3. Use an Ethernet cable to connect the management interface to a protected network segment. The default IP address of the management interface is 192.168.45.45 with a Netmask of 255.255.255.0.
4. Turn on the Defense Center and continue with the next section, "Setting the IP Address for the Management interface" on page 26.

**Figure 6 TPS 2070 DC rear view**




***NOTE:*** The Management interface corresponds to the eth0 Linux software interface and there are no sensing interfaces on the Defense Center. The unlabeled interface on the motherboard is not used.

## Setting the IP Address for the Management interface

In this section you set up the network interface that you will use later to administer the Defense Center.

To configure the interface:

1. Connect to the Defense Center in one of the following ways:
   - Connect a monitor and a keyboard to the Defense Center and set the management interface to an IP address on the same subnet as the administration system.

or

   - Create an alias on the administration system that is on the same subnet as the default IP address of the management interface (192.168.45.45) and then access the Defense Center remotely using SSH.
2. Log in as root. The system requests a password.
3. Enter Nortel as the password. The password is case sensitive.

***WARNING!*** Nortel strongly recommends that you change this password before installing the Defense Center in a production environment.

4. To change the password, type passwd then enter the new password for root. Be sure to document the new password.

5. To determine the name of the management interface, enter the following command: grep MANAGEMENT /etc/sf/ims.conf
6. To configure the management interface, enter the following command:

```
ifconfig eth# ipaddr netmask mask broadcast bcastaddr
```

where eth# is the result you received for the command in the previous step, and ipaddr, mask, and `bcastaddr` are the values you want to use in your network environment.

For example:

```
ifconfig eth0 192.168.10.5 netmask 255.255.255.0
broadcast 192.168.10.255
```

7. If the Defense Center is on a different subnet from the web browser, add a default route as shown in the following command:

```
route add default gw gw_addr
```

where gw_addr is the IP address of the default gateway.

For example:

```
route add default gw 192.168.10.1
```

8. Continue with "Performing the initial setup" on page 27.

## Performing the initial setup

After you physically install the Defense Center and set up the IP address for the management interface, you must log into the Defense Center's web interface and continue the setup process. After you perform the initial setup, refer to your user guide for information about the next steps you need to take.

See the following sections for more information:


- "Accessing the web interface" on page 27
- "Changing the default password" on page 28
- "Configuring the network settings" on page 28
- "Setting up the base license" on page 30
- "Setting up remote management" on page 30
- "Installing software updates" on page 31
- "Importing SEUs and rule files" on page 31
- "Configuring a system policy" on page 32


### Accessing the web interface

1. Connect to the management interface securely to access the GUI.

   To access the GUI through the management interface, browse to the IP address you configured in the previous procedure, for example, `https://192.168.10.5`.

   The Login page appears.

2. Type **admin** for the login name and **Nortel** for the password and click **Login**.

   The End User License Agreement screen appears.

3. Read the agreement and, if you agree to follow the license agreement, click **Agree**.

   The Change Password page appears.

Continue with "Changing the default password" on page 28.

### Changing the default password

You must select a new password for the admin user account.

To change the default password:

1. In the Current Password field, type your current password (Nortel).
2. In the New Password and Confirm fields, type your new password.

---

***IMPORTANT!*** Make sure you select a password that conforms to your security policies, and ensure that only appropriate personnel have access to this user account and password.

---

3. Click **Change**. The password is changed and you can continue with "Configuring the network settings" on page 28.

---

***TIP!*** You can obtain online help for each of the initial setup pages by clicking the Help icon at the top of the page.

---

### Configuring the network settings

You can choose to use DHCP network settings or static network settings for the Defense Center. If you specify the DHCP option, the Defense Center will automatically retrieve its network settings from a local DHCP server. If you specify the Static option, you must manually configure all network properties.

If the Defense Center is not directly connected to the Internet, you can configure a proxy server to be used when downloading updates. By default, the Defense Center is configured to directly connect to the Internet.

---

***TIP!*** To use the default settings, click Skip Configuration and continue with "Setting up the base license" on page 30.

---

To configure your network settings:

1. Specify how you want to configure network settings:
   - Select Use DHCP to use DHCP network setting resolution.

- Select Use Static to manually specify network settings. The following table provides a description of each field you can configure.

**Network settings**

| Settings | Description |
|---|---|
| Management Interface and Netmask | The IP address and network mask for the management interface.<br><br>In most installations, the management interface is connected to an internal, protected network. This is the IP address that Defense Centers and sensors communicate through. Also, this is the IP address for the Defense Center's user interface. |
| Default Network Gateway | The IP address of the gateway device for your network. |
| Hostname | The DNS-resolvable name for the 3D Sensor |
| Domain | The fully qualified domain name where the Defense Center resides. |
| Primary DNS Server | The IP address of your DNS server for the network where the Defense Center resides. |
| Secondary DNS Server | A secondary DNS server's IP address. |

***IMPORTANT!*** If you change the hostname, the new name is not reflected in the syslog until after you reboot the Defense Center.

2. By default, the Defense Center is configured to connect directly to the Internet. If the Defense Center is not directly connected to the Internet, you can identify a proxy server to be used when downloading updates and rules.

Select Manual proxy configuration and enter the IP address or fully qualified domain name of your proxy server in the HTTP Proxy field and the port in the Port field.

3. You have two options:

- If you made any changes to the network settings or proxy configuration, click Reconfigure.

The configuration is changed based on your settings. If necessary, you can log in again with the admin account and continue with “Setting up the base license” on page 30.

- If you are using DHCP to specify your network settings, click Skip Configuration.

---

***IMPORTANT!*** If you restored your appliance to factory specifications, but you were able to retain your network settings and license file, you can use the Restore Saved Settings option to refresh the page with your saved network settings if you make an error on the page.

---

### Setting up the base license

The top of the Manage License page includes a unique license key that you must use to request a license file for your Defense Center. Each appliance has its own license key and requires its own license file. The process for obtaining the license key requires a host with a web browser that can access the Internet.

To set up the base license:

1. After you obtain the license, paste it into the License field, and click Submit License.

### Setting up remote management

The Defense Center uses a range of internal network IP addresses to transmit third-party communications such as NTP to managed sensors and, in high availability deployments, to its Defense Center peer.

The default address range is 172.16.0.0/16. If the IP address range or the port conflicts with other communications on your network, you can specify different values. The default port for all communications between the Defense Center, its managed sensors, and if high availability is enabled, its high availability peer is 8305/tcp.

---

***TIP!*** To use the default settings, click Save and continue with "Configuring a system policy" on page 32.

---

To configure the communications channel on a Defense Center:

1. On the System Settings page, in the Management Port field, enter the port number that you want to use.

---

***WARNING!*** If you change the management port during the initial setup for any appliance in your deployment, make sure you change the port on all the appliances.

---

2. In the Management Virtual Network field, enter the IP address range that you want to use, in CIDR notation.
3. Click Save to save your changes for both the IP address range and the port number.

The new values are saved and you can continue with “Installing software updates” on page 31.

### Installing software updates

If an update is available for your Defense Center, use the Patch Update Management page to update your system.

***TIP!*** If no software update is available, click Continue and skip to “Importing SEUs and rule files” on page 31.

To install an update:

1. Upload the update to the Defense Center in one of two ways:
   - If your Defense Center has access to the Internet, click Update to check for the latest updates on the Support site.

***WARNING!*** Make sure you upload updates directly from the Support site or by clicking Update. Do not transfer them by email, as they may become corrupted during transmission.

2. Under Updates, select the update that you want to apply and click Install. If you are installing an update that requires a system reboot, you must confirm that you want to restart the system.

The update is installed and you can click Continue to continue with “Importing SEUs and rule files” on page 31.

### Importing SEUs and rule files

If you licensed the IPS component, you can import the latest version of the Security Enhancement Update (SEU). SEUs contain new and updated standard text rules and shared object rules that you can use to detect potential attacks against your network and its assets. In addition, an SEU can also provide IPS with an updated version of Snort, as well as features such as new preprocessors and decoders.

***IMPORTANT!*** SEUs can contain new binaries. Make sure your process for uploading and installing SEUs complies with your security policies.

***TIP!*** If no SEU update is available, click Continue and continue with “Configuring a system policy” on page 32.

To install an SEU:

1. Specify how you want to set the rule state for new rules after import:
   - If you want any new rules to use the default rule state set by Nortel in your existing policies, select In the default state.
   - If you want to disable new rules, select In the disabled state.
2. You can upload the SEU to the Defense Center in one of two ways:
   - If your Defense Center has access to the Internet, select Download new SEU (from the support site), then click Update.

---

***WARNING!*** Make sure you upload the SEU directly from the Support site or by clicking Update. Do not transfer them by email, as it may become corrupted during transmission.

---

The SEU is updated and you can click Continue to continue with "Configuring a system policy" on page 32.

### Configuring a system policy

A system policy controls various aspects of an appliance. As part of the initial setup, you can configure the default system policy and automatically apply it to your Defense Center.

---

***TIP!*** To use the default settings, click Skip to complete the initial setup and display the start page for your Defense Center.

---

To configure the default system policy:

Select a link on the left side of the page to move between the pages in the system policy, making changes as needed. You can click Save Policy and Continue at any point in the process to save the changes you already made and use the default settings for the remainder of the options. The start page for your Defense Center appears.

## Console output

Please note that DC 4.7.0 installation output redirects to serial and not to the console.

# 3D SENSOR 2x50/2x70

The Nortel TPS 3D Sensor 2x50 and Nortel TPS 3D Sensor 2x70 offer the flexibility to modify existing rules, tune the rule set, and create custom rules. They provide quick snapshots of exploits against a network and save detailed packet information showing TCP/IP headers and payload. When specific attack data is analyzed, the user is able to easily search the event and packet data in the database.

3D Sensor 2x50 and 3D Sensor 2x70 deliver high-quality, real-time intrusion detection as well as:

- comprehensive attack recognition
- rules written in the Snort rules language
- configurable rules and preprocessors

See the following sections for more information about installing a 3D Sensor:

- "Security considerations" on page 33
- "Installing the 3D Sensor 2x50/2x70" on page 33
- "Setting the IP Address for the Management Interface" on page 35
- "Performing the initial setup" on page 36
- "Console output" on page 42

## Security considerations

Before installing the 3D Sensor 2x50/2x70, Nortel recommends the following:

- Place the 3D Sensor in a lockable rack within a secure location that prevents access by unauthorized personnel. If installing a desktop model, place it within a secure location that prevents access by unauthorized personnel.
- Allow only trained and qualified personnel to install, replace, administer, or service the 3D Sensor.
- Always connect the management interface to a secure internal management network that is protected from unauthorized access

## Installing the 3D Sensor 2x50/2x70

To install the 3D Sensor do the following:

---

***TIP!*** The 3D Sensor is delivered on different hardware appliances. Refer to the correct illustration for the appliance while following the installation procedure.

---

To install the appliance:

1. Using the enclosed mounting kit, mount the 3D Sensor in the rack.
2. Attach the power cord to the 3D Sensor. Plug it in to a power source.

***IMPORTANT!*** If your 3D Sensor has redundant power supplies, attach power cords to both power supplies and plug them in.

3. Use an Ethernet cable to connect the management interface to a protected network segment.

   The default IP address of the management interface is 192.168.45.45 with a Netmask of 255.255.255.0

4. Turn on the 3D Sensor and continue with the next section, "Setting the IP Address for the Management Interface" on page 35.

**Figure 7 TPS 3D Sensor 2x50 rear view**

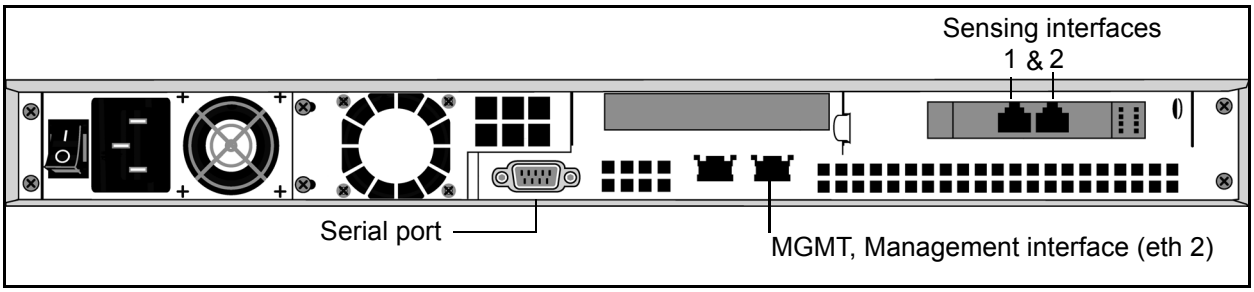
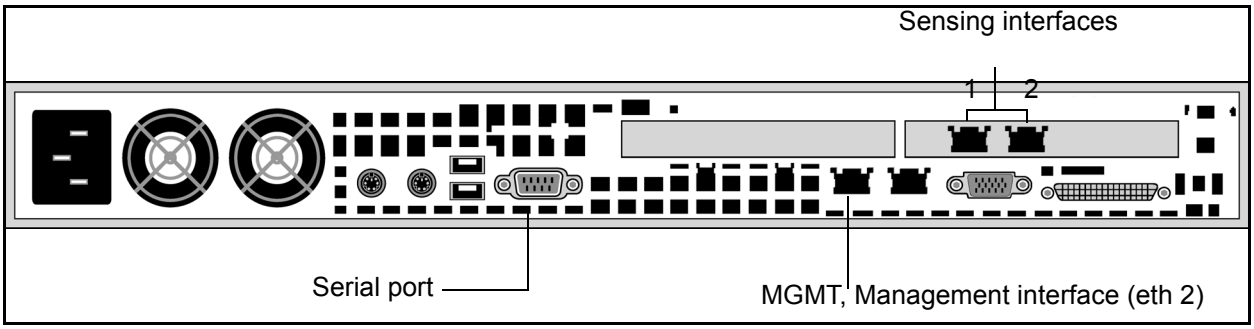



**Figure 8 TPS 3D Sensor 2x70 rear view**




***IMPORTANT!*** The Management Interface corresponds to the eth2 Linux software interface. Sensing interfaces 1 and 2, and the unlabeled interface on the motherboard, are all part of the bond0 Linux software interface.

## Setting the IP Address for the Management Interface

In this section you set up the network interface that you will use later to administer the 3D Sensor.

To configure the interface:

1. Connect to the 3D Sensor in one of the following ways:
   - Connect a monitor and a keyboard to the 3D Sensor and set the management interface to an IP address on the same subnet as the administration system.
   - Create an alias on the administration system that is on the same subnet as the default IP address of the management interface (192.168.45.45) and then access the 3D Sensor remotely using SSH.
2. Log in as root. The system requests a password.
3. Enter **Nortel** as the password.

   ***TIP!*** Note that the password is case sensitive.

   ***WARNING!*** Nortel strongly recommends that you change this password before installing the 3D Sensor in a production environment.

4. To change the password, type `passwd` then enter the new password for root. Be sure to document the new password.
5. To determine the name of the management interface, enter the following command:

   ```
   grep MANAGEMENT /etc/sf/ims.conf
   ```

6. To configure the management interface, enter the following command:

   ```
   ifconfig eth# ipaddr netmask mask broadcast bcastaddr
   ```

   where `eth#` is the result you received for the command in the previous step, and `ipaddr`, `mask`, and `bcastaddr` are the values you want to use in your network environment. For example:

   ```
   ifconfig eth0 192.168.10.5 netmask 255.255.255.0
   broadcast 192.168.10.255
   ```

7. If the 3D Sensor is on a different subnet from the web browser, add a default route as shown in the following command:

   ```
   route add default gw gw_addr
   ```

   where `gw_addr` is the IP address of the default gateway. For example:

   ```
   route add default gw 192.168.10.1
   ```

8. Continue with “Performing the initial setup” on page 36.

## Performing the initial setup

After physically installing the 3D Sensor and setting up the IP address for the management interface, the user must log into the 3D Sensor's web interface and continue the setup process. After performing the initial setup, refer to the user guide for information for the next steps.

See the following sections for more information:


- "Accessing the web interface" on page 36
- "Changing the default password" on page 37
- "Configuring the network settings" on page 37
- "Setting up the base license" on page 38
- "Setting up remote management" on page 39
- "Installing software updates" on page 39
- "Importing SEUs and rule files" on page 40
- "Choosing default or custom interface sets and detection engines" on page 41
- "Creating an intrusion policy" on page 41
- "Applying an intrusion policy" on page 42
- "Configuring a system policy" on page 42


### Accessing the web interface

1. Connect to the management interface securely to access the GUI. To access the GUI through the management interface, browse to the IP address configured in "Setting the IP Address for the Management Interface" on page 35, for example,

   `https://192.168.10.5/.`

   The Login page appears.
2. Type **`admin`** for the login name and **`Nortel`** for the password.
3. Click Login. The End User License Agreement (EULA) screen appears.
4. Read the agreement and, click Agree to proceed. The Change Password page appears. Continue with "Changing the default password" on page 37.

### Changing the default password

You must select a new password for the admin user account. To change the default password:

1. In the Current Password field, type your current password (**`Nortel`**).
2. In the New Password and Confirm fields, type your new password.

---

***IMPORTANT!*** Make sure to select a password that conforms to your security policies, and ensure that only appropriate personnel have access to this user account and password.

---

3. Click Change. The password is changed. Continue with "Configuring the network settings" on page 37.

   You can obtain online help for each of the initial setup pages by clicking the Help icon at the top of the page.

### Configuring the network settings

You can choose to use DHCP network settings or static network settings for the Defense Center. If you specify the DHCP option, the 3D Sensor will automatically retrieve its network settings from a local DHCP server. If you specify the Static option, you must manually configure all network properties. If the 3D Sensor is not directly connected to the Internet, you can configure a proxy server to be used when downloading updates. By default, the 3D Sensor is configured to directly connect to the Internet.

---

***TIP!*** To use the default settings, click Skip Configuration and continue with "Setting Up the Base License."

---

To configure your network settings:

1. Specify how you want to configure network settings:
   - Select Use DHCP to use DHCP network setting resolution.
   - Select Use Static to manually specify network settings. The following table provides a description of each field you can configure.

| Setting | Description |
|---|---|
| Management Interface and Netmask | The IP address and network mask for the management interface. |
| Default Network Gateway | The IP address of the gateway device for your network. |
| Hostname | The DNS-resolvable name for the 3D Sensor |

***IMPORTANT!*** If you change the hostname, the new name is not reflected in the syslog until after you reboot the 3D Sensor. Domain The fully qualified domain name where the 3D Sensor resides. Primary DNS Server The IP address of your DNS server for the network where the 3D Sensor resides. Secondary DNS Server A secondary DNS server's IP address.

2. By default, the 3D Sensor is configured to connect directly to the Internet. If the 3D Sensor is not directly connected to the Internet, you can identify a proxy server to be used when downloading updates and rules. Select Manual proxy configuration and enter the IP address or fully qualified domain name of your proxy server in the HTTP Proxy field and the port in the Port field.
3. You have two options:
   - If you made any changes to the network settings or proxy configuration, click Reconfigure. The configuration is changed based on your settings. If necessary, you can log in again with the admin account and continue with "Setting Up the Base License."
   - If you are using DHCP to specify your network settings, click Skip Configuration. Your settings are saved and you can continue with "Setting Up the Base License."

***IMPORTANT!*** If you restored your appliance to factory specifications, but you were able to retain your network settings and license file, you can use the Restore Saved Settings option to refresh the page with your saved network settings if you make an error on the page.

### Setting up the base license

The top of the Manage License page includes a unique license key that you must use to request a license file for your 3D Sensor. Each appliance has its own license key and requires its own license file. The process for obtaining the license key requires a host with a web browser that can access the Internet.

To set up the base license:

1. After you obtain the license, paste it into the License field, and click Submit License.

### Setting up remote management

1. In the Management Host field, type the IP address or the hostname of the Defense Center that you want to use to manage the sensor.

   ***WARNING!*** Make sure you use host names rather than IP addresses if your network uses DHCP to assign IP addresses.

2. Optionally, in the Registration ID field, type a unique alphanumeric registration ID that you want to use to identify the sensor.

   ***TIP!*** This is especially useful in a network environment that uses network address translation and more than one sensor could have the same IP address.

3. In the Registration Key field, type the one-time use registration key that you want to use to set up a communications channel between the sensor and the Defense Center.
4. Click Save. The sensor will begin communicating with the Defense Center.

After you finish setting up the sensor, configure Remote Access to the Defense Center to set up the communications from the Defense Center to the sensor.Continue with setting up the management port.

To set up the management port on a 3D Sensor:

5. In the Management Port field, enter the port number that you want to use.

   ***WARNING!*** If you change the management port during the initial setup for any appliance in your deployment, make sure you change the port on all managed sensors and the high availability peer, if applicable. Click Save to continue with “Configuring a System Policy”

### Installing software updates

If an update is available for your 3D Sensor, use the Patch Update Management page to update your system.

***TIP!*** If no software update is available, click Continue and skip to “Importing SEUs and rule files” on page 40.

To install an update:

1. Upload the update to the 3D Sensor in one of two ways:
   - If your 3D Sensor has access to the Internet, click Update to check for the latest updates on the Support site.

   ***WARNING!*** Make sure you upload updates directly from the Support site or by clicking Update. Do not transfer them by email, as they may become corrupted during transmission.

2. Under Updates, select the update that you want to apply and click Install. If you are installing an update that requires a system reboot, you must confirm that you want to restart the system. The update is installed and you can click Continue to continue with "Importing SEUs and rule files" on page 40.

### Importing SEUs and rule files

If you licensed the IPS component, you can import the latest version of the Security Enhancement Update (SEU). SEUs contain new and updated standard text rules and shared object rules that you can use to detect potential attacks against your network and its assets. In addition, an SEU can also provide IPS with an updated version of Snort, as well as features such as new preprocessors and decoders.

***IMPORTANT!*** SEUs can contain new binaries. Make sure your process for uploading and installing SEUs complies with your security policies.

***TIP!*** If no SEU update is available, click Continue and continue with "Configuring a System Policy."

To install an SEU:

1. Specify how you want to set the rule state for new rules after import:
   - If you want any new rules to use the default rule state set by Nortel in your existing policies, select In the default state.
   - If you want to disable new rules, select In the disabled state.
2. You can upload the SEU to the Defense Center in one of two ways:
   - If your Defense Center has access to the Internet, select Download new SEU (from the support site), then click Update.

   ***WARNING!*** Make sure you upload the SEU directly from the Support site or by clicking Update. Do not transfer them by email, as it may become corrupted during transmission. The SEU is updated and you can click Continue to continue with "Configuring a system policy" on page 42.

### Choosing default or custom interface sets and detection engines

Depending on the hardware configuration of your 3D Sensor, applicable Interface sets are displayed in the drop-down list. You can choose to use a default interface set and detection engine or build a custom interface set and detection engine.

choose:

- Custom to build a custom interface set and a detection engine.

---

***IMPORTANT!*** An interface set and a detection engine are required for proper 3D Sensor operation. If you choose Custom you must create an interface set and detection engine by selecting the Create function at the empty Interface Set List and empty Detection Engine List pages.

---

- Passive with RNA to build a single IPS interface set with RNA for all 3D Sensor interfaces.
- Passive without RNA to build a single IPS interface set for all 3D Sensor interfaces.
- Inline with Fail-Open with RNA, to build paired fail-open IPS interface sets on all 3D Sensor interfaces.
- Inline with Fail-Open without RNA, to build paired fail-open IPS interface sets on all 3D Sensor interfaces.
- Click Save when your choice is made.

### Creating an intrusion policy

Two default passive policies and three default inline intrusion are delivered with the Nortel Threat Protection System. By using the policies provided by Nortel as a basis for your intrusion policy, you can take advantage of the experience of the VRT. Default rule sets include:

- Passive - Default Policy (provided by Nortel)
- No Rules Active (provided by Nortel)
- Security over Connectivity (provided by Nortel)
- Connectivity over Security (provided by Nortel)
- Balanced Security and Connectivity (provided by Nortel)

To copy and use one of the default policies:

1. Use the Copy Policy drop-down list to select the policy on which you want to base the new policy. You can select any of the default Nortel intrusion policies or any user-defined policy as the basis for your new policy.
2. Type a name and description for the policy.

3. Select Passive or InLine from the Policy Mode drop-down list, as appropriate.

***TIP!*** Note that your policy becomes available, but does not take effect until you apply it to a detection engine. Click Save and continue with "Applying an intrusion policy" on page 42.

### Applying an intrusion policy

The Detection and Prevention page appears without a policy during initial startup. Click Create Policy to create a new intrusion policy. After the intrusion policy is created, the detection and prevention policy name page is displayed. Click Apply. next to the policy you want to use.

### Configuring a system policy

A system policy controls various aspects of an appliance. As part of the initial setup, you can configure the default system policy and automatically apply it to your 3D Sensor.

***TIP!*** To use the default settings, click Skip to complete the initial setup and display the start page for your Defense Center.

To configure the default system policy:

1. Select a link on the left side of the page to move between the pages in the system policy, making changes as needed. You can click Save Policy and Continue at any point in the process to save the changes you already made and use the default settings for the remainder of the options. The start page for your 3D Sensor appears.

## Console output

Please note that 3D Sensor 4.7.0 installation output redirects to serial and not to the console.

# CHAPTER 3
# HARDWARE SPECIFICATION

This chapter provides the hardware specifications for the following TPS appliances:

- TPS 3D Sensor 2050
- TPS 3D Sensor 2070
- TPS 3D Sensor 2150
- TPS 3D Sensor 2170
- TPS 2070 DC

# TPS 2x50 3D Sensor

The Nortel TPS 3D Sensor 2050 and TPS 3D Sensor 2150 are designed to maximize performance in a 1U format.

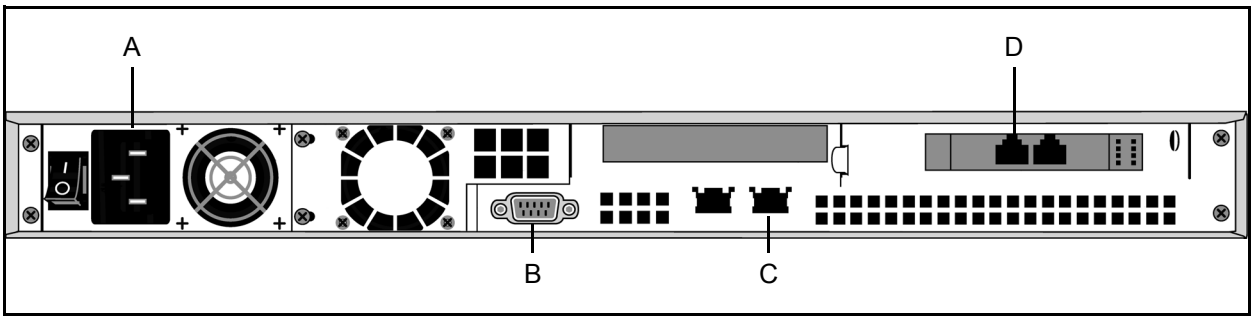
See the following sections for a complete description of the TPS 3D Sensor 2050 and the TPS 3D Sensor 2150:

- ”Chassis back I/O ports and features”
- “Chassis front features” on page 45
- “Chassis dimensions” on page 45
- “System operating environment” on page 46
- “Rack and cabinet mounting options” on page 46

## Chassis back I/O ports and features

Figure 9 shows the ports on the back of the TPS 3D Sensor 2050 and TPS 3D Sensor 2150 chassis.

**Figure 9 TPS 2x50 3D Sensor chassis rear view**

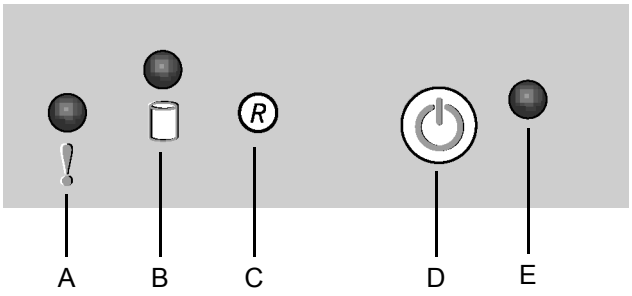



| | |
|---|---|
| **A** | Power connector |
| **B** | DB-9 DCE serial connector |
| **C** | 10/100/1000 RJ-45 Ethernet connector |
| **D** | Expansion card with 10/100/1000 RJ-45 Ethernet connectors |

## Chassis front features

Figure 10 illustrates the features on the front of the chassis.

**Figure 10 TPS 2x50 3D Sensor chassis front view**




| | |
|---|---|
| **A** | System status indicator<br><br>The amber system status LED lights up when the system needs attention due to a problem with power supplies, fans, system temperature, or hard drives. |
| **B** | Hard drive status indicator<br><br>This LED blinks when activity is detected on the hard-disk drive. |
| **C** | Reset button |
| **D** | Power button. |
| **E** | Power LED<br><br>This LED is green when the power supply is turned on. |

## Chassis dimensions

The Chassis Dimensions table lists the dimensions of the sensor chassis.

**Chassis Dimensions**

| Dimension | Metric | Imperial |
|---|---|---|
| Height | 43 mm | 1.72 inches |
| Width | 430 mm | 16.9 inches |
| Depth | 559 mm | 22 inches |

## System operating environment

This section describes the required office environment for this version of the TPS 3D Sensor 2050 and the TPS 3D Sensor 2150.

### Environmental parameters

Keep the TPS 3D Sensor 2050 or the TPS 3D Sensor 2150 in an environment that meets the specifications in the Environmental Parameters table.

**Environmental Parameters**

| Parameter | Limits |
|---|---|
| Operating temperature | 5°C to 35°C (41°F to 95°F) |
| Non-operating temperature | -20°C to +80°C (-4°F to +176°F) |
| Operating humidity | 10% to 90% non-condensing |
| Altitude | -16 to 3048 meters (-50 to 10,000 feet) |

## Power supply

The sensor power supply is rated for 300 watts.

## Rack and cabinet mounting options

The TPS 3D Sensor 2050 or the TPS 3D Sensor 2150 can be used in racks and server cabinets that are 19 inches wide and up to 30 inches deep. The sensor comes with a rack-mount kit. Refer to the instructions that are supplied with the sensor for more information about correctly mounting the chassis in a rack.

# TPS 2x70 3D Sensor

The Nortel TPS 3D Sensor 2070 and the TPS 3D Sensor 2170 are designed to maximize performance in a 1U format.

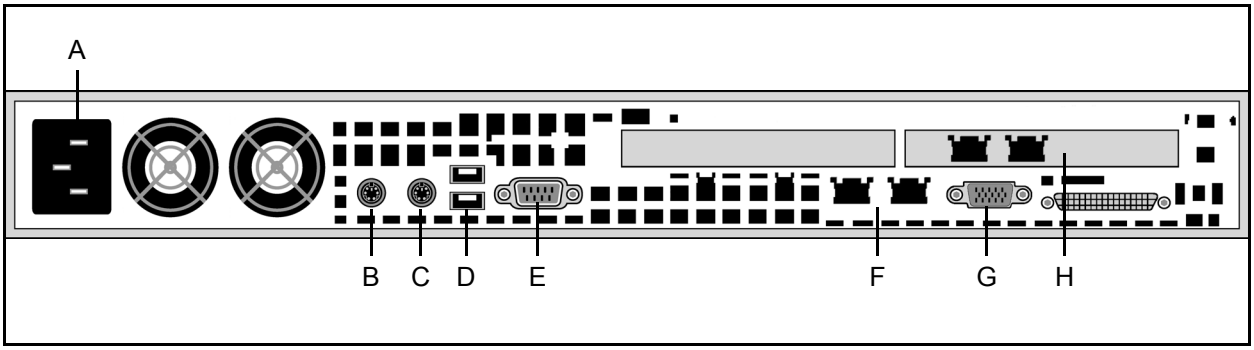
See the following sections for a complete description of the TPS 3D Sensor 2070 and the TPS 3D Sensor 2170:


- ”Chassis back I/O ports and features”
- “Chassis front features” on page 48
- “Chassis dimensions” on page 49
- “System operating environment” on page 49
- “Rack and cabinet mounting options” on page 49


## Chassis back I/O ports and features

Figure 11 shows the ports on the back of the Nortel TPS 3D Sensor 2070 and the Nortel TPS 3D Sensor 2170 chassis.

**Figure 11 TPS 2x70 3D Sensor chassis rear view**

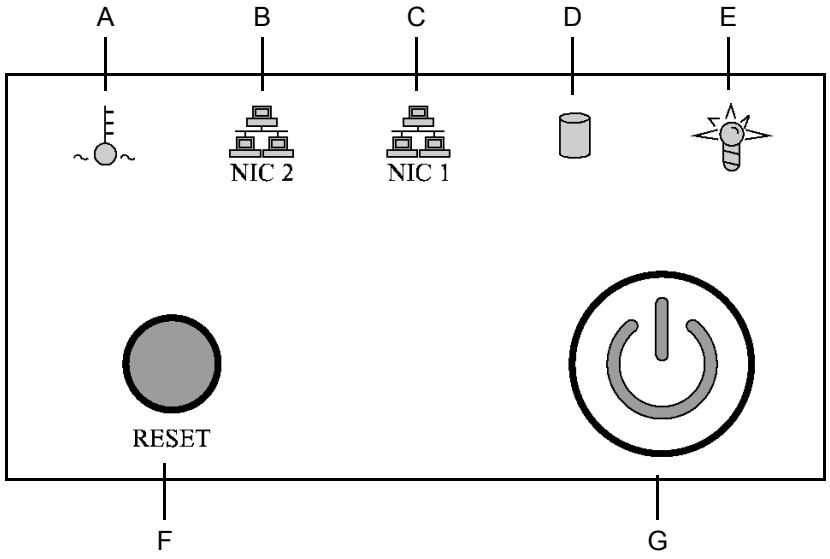



| | |
|---|---|
| **A** | Power connector |
| **B** | Keyboard connector |
| **C** | Mouse connector |
| **D** | USB connectors |
| **E** | DB-9 serial connector |
| **F** | 10/100/1000 RJ-45 Ethernet connectors |
| **G** | Video connector |
| **H** | Expansion card with 10/100/1000 RJ-45 Ethernet connectors |

## Chassis front features

Figure 12 illustrates the features on the front of the TPS 3D Sensor 2070 and the TPS 3D Sensor 2170 chassis.

**Figure 12 TPS 2x70 3D Sensor chassis front view**




| | |
|---|---|
| **A** | Overheat indicator<br><br>This LED is red when the system overheats. |
| **B** | NIC 2 indicator<br><br>This LED is steady green when linked and blinks to show network activity. |
| **C** | NIC 1 indicator<br><br>This LED mirrors the state of the Link/Act LED of the Management port. It is steady green when linked and blinks to show network activity. |
| **D** | Hard drive status indicator<br><br>This LED is amber and blinks when activity is detected on the hard disk drive. |
| **E** | Power LED<br><br>This LED is green when the power supply is turned on. |
| **F** | Reset button |
| **G** | Power button |

## Chassis dimensions

The Chassis Dimensions table lists the dimensions of the chassis.

**Chassis Dimensions**

| Dimension | Metric | Imperial |
|---|---|---|
| Height | 43 mm | 1.7 inches |
| Width | 445 mm | 16.7 inches |
| Depth | 574 mm | 25.6 inches |

## System operating environment

This section describes the required office environment for the TPS 3D Sensor 2070 and the TPS 3D Sensor 2170.

### Environmental parameters

Keep the TPS 3D Sensor 2070 or the TPS 3D Sensor 2170 in an environment that meets the specifications in the Environmental Parameters table.

**Environmental Parameters**

| Parameter | Limits |
|---|---|
| Operating temperature | 10°C to 35°C (50°F to 95°F) |
| Non-operating temperature | -40°C to +70°C (-40°F to +158°F) |
| Operating humidity | 8% to 90% non-condensing |

## Power supply

The sensor power supply is rated for 400 watts.

## Rack and cabinet mounting options

The TPS 3D Sensor 2070 or the TPS 3D Sensor 2170 can be used in racks and server cabinets that are 19 inches wide and up to 30 inches deep. The sensor comes with a rack-mount kit. Refer to the instructions that are supplied with the sensor for more information about correctly mounting the chassis in a rack.

# TPS 2070 DC

The Nortel TPS 2070 DC is designed to maximize performance in a 1U format.

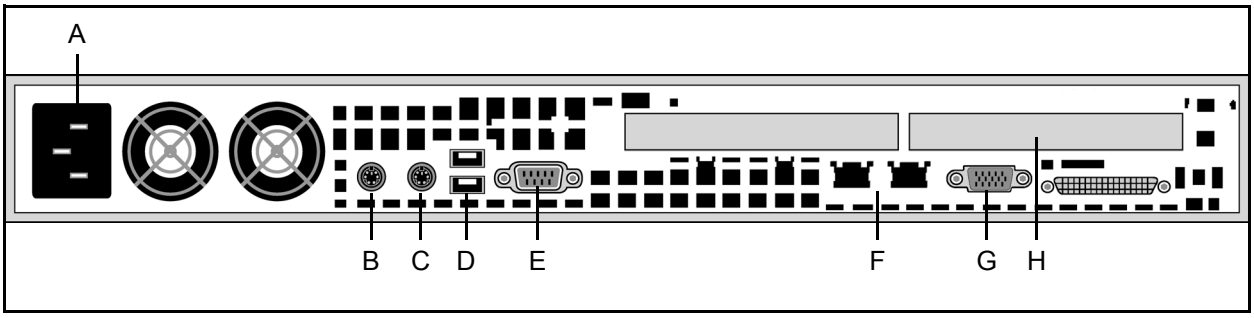
See the following sections for a complete description of the TPS 2070 DC:

- ”Chassis back I/O ports and features”
- “Chassis Front Features” on page 51
- “Chassis dimensions” on page 52
- “System operating environment” on page 52
- “Rack and cabinet mounting options” on page 52

## Chassis back I/O ports and features

Figure 13 shows the ports on the back of the Nortel TPS 2070 DC chassis.

**Figure 13 TPS 2070 DC chassis rear view**

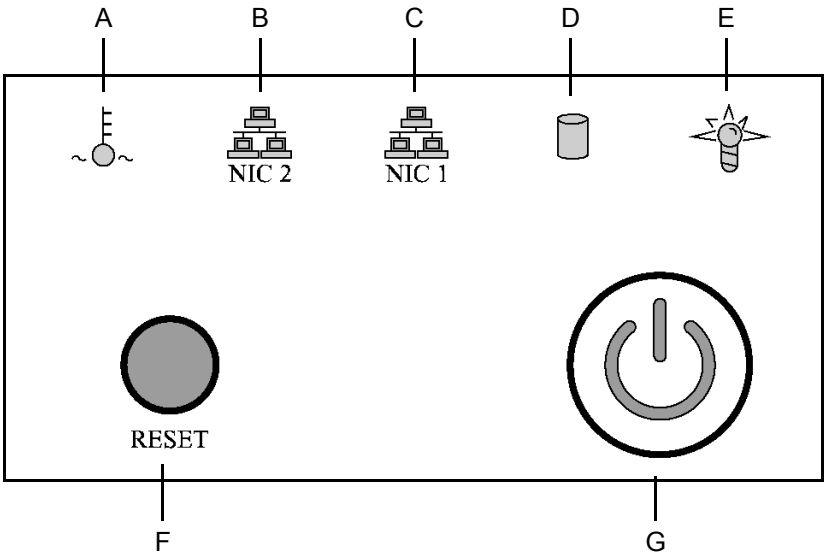



| | |
|---|---|
| **A** | Power connector |
| **B** | Keyboard connector |
| **C** | Mouse connector |
| **D** | USB connectors |
| **E** | DB-9 serial connector |
| **F** | 10/100/1000 RJ-45 Ethernet connectors |
| **G** | Video connector |
| **H** | Expansion slot |

## Chassis Front Features

Figure 14 shows the features on the front of the TPS 2070 DC chassis.

**Figure 14 TPS 2070 DC chassis front features**




| | |
|---|---|
| **A** | Overheat indicator<br><br>This LED is red when the system overheats. |
| **B** | NIC 2 indicator - not used |
| **C** | NIC 1 indicator<br><br>This LED mirrors the state of the Link/Act LED of the Management port. It is steady green when linked and blinks to show network activity. |
| **D** | Hard drive status indicator<br><br>This LED is amber and blinks when activity is detected on the hard disk drive. |
| **E** | Power LED<br><br>This LED is green when the power supply is turned on. |
| **F** | Reset button |
| **G** | Power button |

## Chassis dimensions

The Chassis Dimensions table lists the dimensions of the chassis.

**Chassis Dimensions**

| Dimension | Metric | Imperial |
|---|---|---|
| Height | 43 mm | 1.7 inches |
| Width | 445 mm | 16.7 inches |
| Depth | 574 mm | 25.6 inches |

## System operating environment

This section describes the required office environment for the TPS 2070 DC.

### Environmental parameters

Keep the TPS 2070 DC in an environment that meets the specifications in the Environmental Parameters table.

**Environmental Parameters**

| Parameter | Limits |
|---|---|
| Operating temperature | 10°C to 35°C (50°F to 95°F) |
| Non-operating temperature | -40°C to +70°C (-40°F to +158°F) |
| Operating humidity | 8% to 90% non-condensing |

## Power supply

The sensor power supply is rated for 400 watts.

## Rack and cabinet mounting options

The TPS 2070 DC can be used in racks and server cabinets that are 19 inches wide and up to 30 inches deep. The sensor comes with a rack-mount kit. Refer to the instructions that are supplied with the sensor for more information about correctly mounting the chassis in a rack.

# APPENDIX A
# SAFETY AND REGULATORY INFORMATION

The safety warnings and regulatory information for the Nortel Intrusion Sensors and Defense Center are described in the following sections:

- ”Safety information”
- “Regulatory compliance” on page 54

## Safety information

***CAUTION!*** Nortel products are designed to work with single-phase power systems having a grounded neutral conductor. To reduce the risk of electric shock, do not plug Nortel products into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.

***CAUTION!*** Not all power cords have the same ratings. Household extension cords do not have overload protection and are not meant for use with computer systems. Do not use household extension cords with your Nortel Networks product.

***CAUTION!*** Your Nortel product is shipped with a grounding type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.

# Regulatory compliance

## FCC Class A notice

The equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: 1) The device may not cause harmful interference, and 2) This equipment must accept any interference received, including interference that may cause undesired operation.

The equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The equipment generates, uses and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. Operation of this equipment in a residential area is likely to cause harmful interference. In such a case, the user will be required to correct the interference at his own experience.

Do not make mechanical or electrical modifications to the equipment.

## Industry Canada

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe A respecte toutes les exigences du Reglements sur le materiel brouilleur du Canada.

## Japanese VCCI Class A notice

This is a Class A product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur. In such a case, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

## Taiwan EMC statement

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## CE notice

The CE mark on this equipment indicates that this equipment meets or exceeds the following technical standards: EN50082-1, EN55022, EN60555-2, EN61000-4-1, EN61000-4-2, EN61000-4-3, EN61000-4-4, and EN61000-4-5.

# Installation Guide
# Nortel TPS 3D Sensor and Defense Center



Release 4.7.0

Publication: NN47240-300 (320737-B)
Document status: Standard
Document revision: 01.01
Document release date: 3 December, 2007

To provide feedback, or to report a problem in this document, go to www.nortel.com/documentfeedback.



NORTEL