Deploying Virtual Appliances

Using virtual devices and virtual Defense Centers allows you to deploy security solutions within your virtual environment for increased protection of both physical and virtual assets. Virtual devices and virtual Defense Centers enable you to easily implement security solutions on the VMware platform. Virtual devices also make it easier to deploy and manage devices at remote sites where resources may be limited.

In these examples, you can use a physical or virtual Defense Center to manage your physical or virtual devices. You can deploy on a IPv4 or IPv6 network. You can also configure multiple management interfaces on the Defense Center to isolate and monitor two different networks, or to separate internal and event traffic on a single network. Note that virtual devices do not support multiple management interfaces.

You can configure a second management interface on your virtual Defense Center to improve performance or to manage traffic separately on two different networks. Configure an additional interface and an additional virtual switch to connect the second management interface to a managed device on the second network. For more information about multiple management interfaces, see Managing Devices in the FireSIGHT System User Guide.

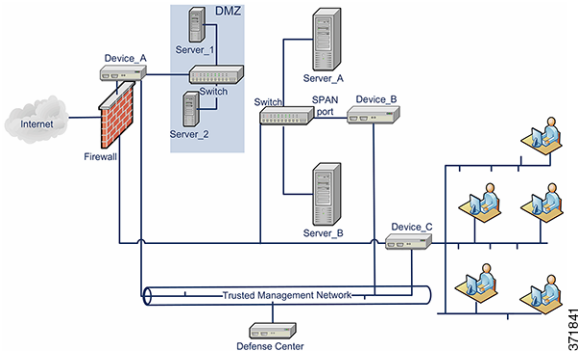
To add a second management interface to your virtual appliance, see VMware vSphere (http://vmware.com).

Caution Cisco **strongly** recommends that you keep your production network traffic and your trusted management network traffic on different network segments. You must take precautions to ensure the security of the appliances and the management traffic data stream.

This chapter provides deployment examples for:

Typical FireSIGHT System Deployment

In a physical appliance environment, a typical FireSIGHT System deployment uses physical devices and a physical Defense Center. The following graphic displays a sample deployment. You can deploy Device_A and Device_C in an inline configuration and Device_B in a passive configuration, as shown below.



You can configure port mirroring on most network switches to send a copy of network packets seen on one switch port (or an entire VLAN) to a network monitoring connection. Also called Switch Port Analyzer or SPAN by a major network equipment provider, port mirroring allows you to monitor network traffic. Note that Device_B monitors the traffic between Server_A and Server_B via a SPAN port on the switch between Server_A and Server_B.

VMware Virtual Appliance Deployments

See the following set of virtual appliance deployment scenarios for examples of typical deployments:

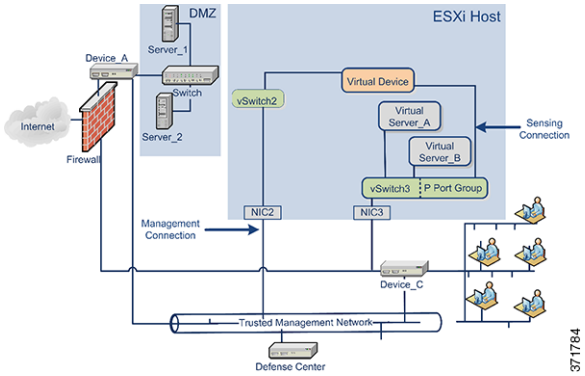
- Adding Virtualization and a Virtual Device, page 3-2
- Using the Virtual Device for Inline Detection, page 3-3
- Adding a Virtual Defense Center, page 3-4
- Using a Remote Office Deployment, page 3-5

Adding Virtualization and a Virtual Device

You can replace the physical internal servers in our Typical FireSIGHT System Deployment, page 3-1 by using virtual infrastructure. In the following example, you can use an ESXi host and virtualize Server_A and Server_B.

You can use a virtual device to monitor the traffic between Server_A and Server_B.

The virtual device sensing interface must connect to a switch or port group that accepts promiscuous mode traffic, as shown below.



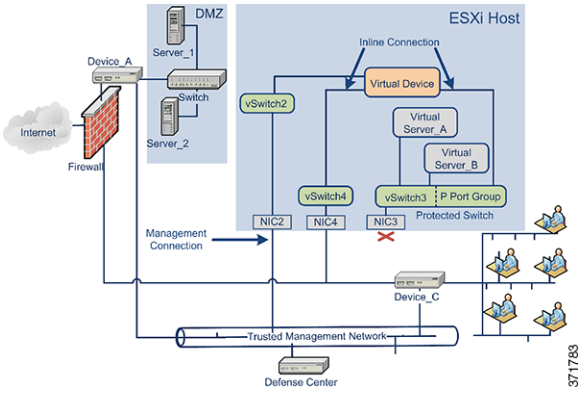
Note To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See Configuring Virtual Device Sensing Interfaces, page 4-10.

Although our example shows only one sensing interface, two sensing interfaces are available by default on your virtual device. The virtual device management interface connects to your trusted management network and your Defense Center.

Using the Virtual Device for Inline Detection

You can provide a secure perimeter around virtual servers by passing traffic through your virtual device's inline interface set. This scenario builds on the Typical FireSIGHT System Deployment, page 3-1 and on the example shown in Adding Virtualization and a Virtual Device, page 3-2.

First, create a protected virtual switch and connect it to your virtual servers. Then, connect the protected switch through your virtual device to the external network. For more information, see the *FireSIGHT System User Guide*.



Note To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See Configuring Virtual Device Sensing Interfaces, page 4-10.

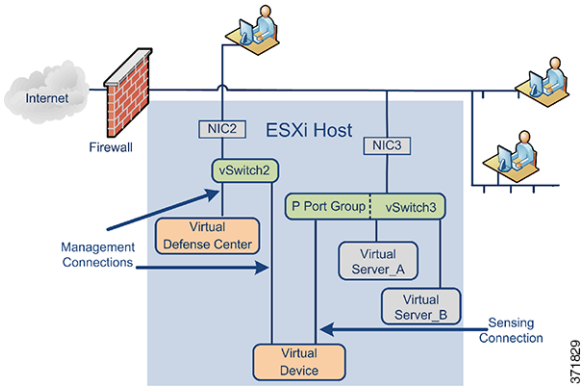
The virtual device monitors and drops any malicious traffic to Server_A and Server_B, depending on your intrusion policy.

Adding a Virtual Defense Center

You can deploy a virtual Defense Center on an ESXi host and connect it to the virtual network as well as the physical network, as shown below. This scenario builds on the Typical FireSIGHT System Deployment, page 3-1 and on the example shown in Using the Virtual Device for Inline Detection, page 3-3.

The connection from a virtual Defense Center through NIC2 to the trusted management network allows the virtual Defense Center to manage both physical and virtual devices.

Because Cisco virtual appliances are preconfigured with the required application software, they are ready to run when deployed on an ESXi host. This diminishes complex hardware and software compatibility issues so you can accelerate your deployment and concentrate on the benefits of a FireSIGHT System. You can deploy virtual servers, a virtual Defense Center, and a virtual device on an ESXi host and manage the deployment from the virtual Defense Center, as shown below.

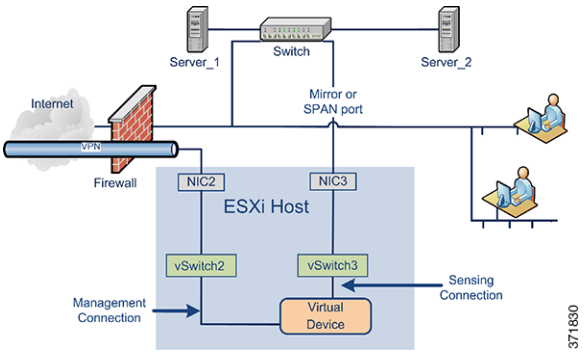


Your sensing connection on your virtual device must be allowed to monitor network traffic. The virtual switch, or the port group on that switch to which the virtual interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In the example, the P Port Group is set to accept promiscuous mode traffic. See Configuring Virtual Device Sensing Interfaces, page 4-10.

Your virtual appliance management connections are more typical, non-promiscuous mode connections. The virtual Defense Center provides command and control for the virtual device. The connection through the ESXi host's Network Interface Card (NIC2 in our example) allows you to access the virtual Defense Center. See Automating Virtual Defense Center Network Settings, page 5-7 and Setting Up a Virtual Device Using the CLI, page 5-3 for information on setting up the virtual Defense Center and the virtual device management connections.

Using a Remote Office Deployment

A virtual device is an ideal way to monitor a remote office with limited resources. You can deploy a virtual device on an ESXi host and monitor local traffic, as shown below.



Your sensing connection on your virtual device must be allowed to monitor network traffic. To do this, the virtual switch, or port group on the switch to which the sensing interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In our example, all of vSwitch3 is set to accept promiscuous mode traffic. VSwitch3 is also connected through NIC3 to the SPAN port so that it can monitor traffic as it passes through the remote office's switch. See Configuring Virtual Device Sensing Interfaces, page 4-10.

Your virtual device must be managed by a Defense Center. The connection through the ESXi host's Network Interface Card (NIC2 in our example) allows you to access the virtual device with a remote Defense Center.

When deploying devices in disparate geographic locations, you must take precautions to ensure the security of the devices and the data stream by isolating the devices from unprotected networks. You can do this by transmitting the data stream from the device over a VPN or another secure tunneling protocol. See Setting Up a Virtual Device Using the CLI, page 5-3 for information on setting up the virtual device management connections.