FireSIGHT Virtual Installation Guide

Version 5.3.1
July 17, 2014

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

Cisco Systems, Inc.
www.cisco.com
Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers
are listed on the Cisco website at
www.cisco.com/go/offices.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

CHAPTER 1

Introduction to Virtual Appliances

The Cisco FireSIGHT® System combines the security of an industry-leading network intrusion protection system with the power to control access to your network based on detected applications, users, and URLs.

Cisco packages 64-bit virtual Defense Centers® and virtual devices for the VMware vSphere and VMware vCloud Director hosting environments. You can deploy 64-bit virtual Defense Centers and 64-bit virtual managed devices to ESXi hosts using a vCenter, or using vCloud Director. The Defense Center provides a centralized management console and database repository for the system. Virtual devices can inspect traffic on virtual or physical networks in either a passive or inline deployment:

- Virtual devices in a passive deployment simply monitor traffic flowing across a network.
- Passive sensing interfaces receive all traffic unconditionally and no traffic received on these interfaces is retransmitted.
- Virtual devices in an inline deployment allow you to protect your network from attacks that might affect the availability, integrity, or confidentiality of hosts on the network. Inline devices can be deployed as a simple intrusion prevention system. You can also configure inline devices to perform access control as well as manage network traffic in other ways.
- Inline interfaces receive all traffic unconditionally, and traffic received on these interfaces is retransmitted unless explicitly dropped by some configuration in your deployment.

Virtual Defense Centers can manage physical devices, Sourcefire Software for X-Series, and Cisco ASA with FirePOWER Services (ASA FirePOWER), and physical Defense Centers can manage virtual devices. However, virtual appliances do not support any of the system's hardware-based features—virtual Defense Centers do not support high availability and virtual devices do not support clustering, stacking, switching, routing, and so on. For detailed information on physical FireSIGHT System appliances, see the *FireSIGHT System Installation Guide*.

This installation guide provides information about deploying, installing, and setting up virtual FireSIGHT System appliances (devices and Defense Centers). It also assumes familiarity with the features and nomenclature of VMware products, including the vSphere Client and VMware vCloud Director web portal.

The topics that follow introduce you to FireSIGHT System virtual appliances:

FireSIGHT System Virtual Appliances

A FireSIGHT System *virtual appliance* is either a traffic-sensing managed *virtual device* or a managing *virtual Defense Center*. For more information, see the following sections:

- Virtual Defense Centers, page 1-2
- Virtual Managed Devices, page 1-2
- Understanding Virtual Appliance Capabilities, page 1-3
- Operating Environment Prerequisites, page 1-5
- Virtual Appliance Performance, page 1-6

Virtual Defense Centers

A Defense Center provides a centralized management point and event database for your FireSIGHT System deployment. Virtual Defense Centers aggregate and correlate intrusion, file, malware, discovery, connection, and performance data, assessing the impact of events on particular hosts and tagging hosts with indications of compromise. This allows you to monitor the information that your devices report in relation to one another, and to assess and control the overall activity that occurs on your network.

Key features of the virtual Defense Center include:

- device, license, and policy management
- event and contextual information displayed in tables, graphs, and charts
- health and performance monitoring
- external notification and alerting
- correlation, indications of compromise, and remediation features for real-time threat response
- custom and template-based reporting

Virtual Managed Devices

Virtual devices deployed on network segments within your organization monitor traffic for analysis. Virtual devices deployed passively help you gain insight into your network traffic. Deployed inline, you can use virtual devices to affect the flow of traffic based on multiple criteria. Depending on model and license, devices:

- gather detailed information about your organization’s hosts, operating systems, applications, users, files, networks, and vulnerabilities
- block or allow network traffic based on various network-based criteria, as well as other criteria including applications, users, URLs, IP address reputations, and the results of intrusion or malware inspections

Virtual devices do **not** have a web interface. You must configure them via console and command line, and you must manage them with a Defense Center.

Caution You cannot update or reimage virtual devices to Version 5.3.1, but a 5.3.1 Defense Center can manage these devices at Version 5.2 or 5.3.

Understanding Virtual Appliance Capabilities

Virtual appliances have many of the capabilities of physical appliances:

- The virtual Defense Center has the same features as a physical Defense Center, except you cannot create high availability pairs of virtual Defense Centers. With a FireSIGHT license, the virtual Defense Center can monitor 50,000 hosts and users.
- Virtual devices have the traffic and blocking analysis capabilities of physical devices. However, they cannot perform switching, routing, VPN, and other hardware-based, redundancy, and resource-sharing features.

Understanding Virtual Defense Center Capabilities

Table 1-1Supported Capabilities for Virtual Defense Centers, page 1-3 matches the major capabilities of the system with virtual Defense Centers, assuming you are managing devices that support those features and have the correct licenses installed and applied.

For a brief summary of the features and licenses supported with virtual appliances, see FireSIGHT System Components, page 1-7 and Licensing Virtual Appliances, page 1-10.

Keep in mind that virtual Defense Centers can manage Series 2, Series 3, ASA FirePOWER, and X-Series devices. Similarly, Series 2 and Series 3 Defense Centers can manage virtual devices. The Defense Center column for device-based capabilities (such as stacking, switching, and routing) indicates whether a virtual Defense Center can manage and configure devices to perform those functions. For example, although you cannot configure VPN on a virtual device, you can use a virtual Defense Center to manage Series 3 devices in a VPN deployment.

Table 1-1 Supported Capabilities for Virtual Defense Centers

Feature or Capability	Virtual Defense Center
collect discovery data (host, application, and user) reported by managed devices and build a network map for your organization	yes
view geolocation data for your network traffic	yes
manage an intrusion detection and prevention (IPS) deployment	yes
manage devices performing Security Intelligence filtering	yes
manage devices performing simple network-based control, including geolocation-based filtering	yes
manage devices performing application control	yes
manage devices performing user control	yes
manage devices that filter network traffic by literal URL	yes
manage devices performing URL filtering by category and reputation	yes
manage devices performing simple file control by file type	yes
manage devices performing network-based advanced malware protection (AMP)	yes
receive endpoint-based malware (FireAMP) events from your FireAMP deployment	yes

Table 1-1 Supported Capabilities for Virtual Defense Centers (continued)

Feature or Capability	Virtual Defense Center
manage device-based hardware-based features: • fast-path rules • strict TCP enforcement • configurable bypass interfaces • tap mode • switching and routing • NAT policies • VPN	yes
manage device-based redundancy and resource sharing: • device stacks • device clusters • Sourcefire Software for X-Series VAP groups • clustered stacks	yes
establish high availability	no
install a malware storage pack	no
connect to an eStreamer, host input, or database client	yes

Understanding Virtual Managed Device Capabilities

Table 1-2Supported Capabilities for Virtual Managed Devices, page 1-4 matches the major capabilities of the system with virtual managed devices, assuming you have the correct licenses installed and applied from the managing Defense Center.

Keep in mind that although you can use any model of Defense Center running Version 5.3.1 of the system to manage any Version 5.2 or 5.3 virtual device, a few system capabilities are limited by the Defense Center model. For example, you cannot use the Series 2 DC500 to manage virtual managed devices performing Security Intelligence filtering, even though virtual managed devices support that capability. For more information, see Understanding Virtual Defense Center Capabilities, page 1-3.

Table 1-2 Supported Capabilities for Virtual Managed Devices

Feature or Capability	Virtual Managed Device
collect discovery data (host, application, and user) reported by managed devices and build a network map for your organization	yes
view geolocation data for your network traffic	yes
network discovery: host, application, and user	yes
intrusion detection and prevention (IPS)	yes
Security Intelligence filtering	yes
access control: basic network control	yes
access control: geolocation-based filtering	yes

Table 1-2 Supported Capabilities for Virtual Managed Devices (continued)

Feature or Capability	Virtual Managed Device
access control: application control	yes
access control: user control	yes
access control: literal URLs	yes
access control: URL filtering by category and reputation	yes
file control: by file type	yes
network-based advanced malware protection (AMP)	yes
Automatic Application Bypass	yes
fast-path rules	no
strict TCP enforcement	no
configurable bypass interfaces	no
tap mode	no
switching and routing	no
NAT policies	no
VPN	no
device stacking	no
device clustering	no
clustered stacks	no
malware storage pack	no
FireSIGHT System-specific interactive CLI	yes
connect to an eStreamer client	no

Operating Environment Prerequisites

You can host 64-bit virtual appliances on the following hosting environments:

- VMware vSphere Hypervisor 5.1
- VMware vSphere Hypervisor 5.0
- VMware vCloud Director 5.1

For help creating a hosting environment, see the VMware ESXi documentation, including VMware vCloud Director and VMware vCenter.

Virtual appliances use Open Virtual Format (OVF) packaging. VMware Workstation, Player, Server, and Fusion do not recognize OVF packaging and are not supported. Additionally, virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware.

The computer that serves as the ESXi host must meet the following requirements:

- It must have a 64-bit CPU that provides virtualization support, either Intel® Virtualization Technology (VT) or AMD Virtualization™ (AMD-V™) technology.
- Virtualization must be enabled in the BIOS settings

- To host virtual devices, the computer must have network interfaces compatible with Intel e1000 drivers (such as PRO 1000MT dual port server adapters or PRO 1000GT desktop adapters).

For more information, see the VMware website: http://www.vmware.com/resources/guides.html.

Each virtual appliance you create requires a certain amount of memory, CPUs, and hard disk space on the ESXi host. Do **not** decrease the default settings, as they are the minimum required to run the system software. However, to improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. The following table lists the default appliance settings.

Table 1-3 Default Virtual Appliance Settings

Setting	Default	Adjustable Setting?
memory	4GB	yes, and for a virtual device you **must** allocate: • 4GB minimum • 5GB to use category and reputation based URL filtering • 6GB to perform Security Intelligence filtering using large dynamic feeds • 7GB to perform URL filtering and Security Intelligence
virtual CPUs	4	yes, up to 8
hard disk provisioned size	40GB (device) 250GB (Defense Center)	no

Virtual Appliance Performance

It is not possible to accurately predict throughput and processing capacity for virtual appliances. A number of factors heavily influence performance, such as the:

- amount of memory and CPU capacity of the ESXi host
- number of total virtual machines running on the ESXi host
- number of sensing interfaces, network performance, and interface speed
- amount of resources assigned to each virtual appliance
- level of activity of other virtual appliances sharing the host
- complexity of policies applied to a virtual device

Tip VMware provides a number of performance measurement and resource allocation tools. Use these tools on the ESXi host while you run your virtual appliance to monitor traffic and determine throughput. If the throughput is not satisfactory, adjust the resources assigned to the virtual appliances that share the ESXi host.

Although Cisco does not support the installation of tools (including VMware Tools) on the guest layer, you may install tools (such as `esxtop` or VMware/third-party add-ons) on the ESXi host to examine virtual performance. However, you must install these tools either on the host or in the virtualization management layer, and not on the guest layer.

FireSIGHT System Components

The sections that follow describe some of the key capabilities of virtual Defense Centers and virtual devices that contribute to your organization's security, acceptable use policy, and traffic management strategy. For information on the additional features supported with Series 2 and Series 3 appliances, see the *FireSIGHT System Installation Guide* and the *FireSIGHT System User Guide*.

Tip Many virtual appliance capabilities are license and user role dependent. Where needed, FireSIGHT System documentation outlines the requirements for each feature and task.

The topics that follow describe some of the key capabilities of the FireSIGHT System that contribute to your organization's security, acceptable use policy, and traffic management strategy:

- FireSIGHT, page 1-7
- Access Control, page 1-7
- Intrusion Detection and Prevention, page 1-8
- File Tracking, Control, and Malware Protection, page 1-8
- Application Programming Interfaces, page 1-9

FireSIGHT

FireSIGHT™ is Cisco's discovery and awareness technology that collects information about hosts, operating systems, applications, users, files, networks, geolocation information, and vulnerabilities, in order to provide you with a complete view of your network.

You can use the Defense Center's web interface to view and analyze data collected by FireSIGHT. You can also use this data to help you perform access control and modify intrusion rule states. In addition, you can generate and track indications of compromise on hosts on your network based on correlated event data for the hosts.

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can traverse your network. An *access control policy* determines how the system handles traffic on your network. You can use a policy that does not include *access control rules* to handle traffic in one of the following ways, using what is called the *default action*:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection
- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only
- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

You can include access control rules in an access control policy to further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule *action*, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

For each access control policy, you can create a custom HTML page that users see when the system blocks their HTTP requests. Optionally, you can display a page that warns users, but also allows them to click a button to continue to the originally requested site.

As part of access control, the Security Intelligence feature allows you to blacklist—deny traffic to and from—specific IP addresses before the traffic is subjected to analysis by access control rules. If your system supports geolocation, you can also filter traffic based on its detected source and destination countries and continents.

Access control includes intrusion detection and prevention, file control, and advanced malware protection. For more information, see the next sections.

Intrusion Detection and Prevention

Intrusion detection and prevention allows you to monitor your network traffic for security violations and, in inline deployments, to block or alter malicious traffic.

Intrusion prevention is integrated into access control, where you can associate an intrusion policy with specific access control rules. If network traffic meets the conditions in a rule, you can analyze the matching traffic with an intrusion policy. You can also associate an intrusion policy with the default action of an access control policy.

An intrusion policy contains a variety of components, including:

- rules that inspect the protocol header values, payload content, and certain packet size characteristics
- rule state configuration based on FireSIGHT recommendations
- advanced settings, such as preprocessors and other detection and performance features
- preprocessor rules that allow you to generate events for associated preprocessors and preprocessor options

File Tracking, Control, and Malware Protection

To help you identify and mitigate the effects of malware, the FireSIGHT System's file control, network file trajectory, and advanced malware protection components can detect, track, capture, analyze, and optionally block the transmission of files (including malware files) in network traffic.

File Control

File control allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols. You configure file control as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

Network-Based Advanced Malware Protection (AMP)

Network-based *advanced malware protection* (AMP) allows the system to inspect network traffic for malware in several types of files. Virtual devices can store detected files for further analysis to a hard drive.

Regardless of whether you store a detected file, you can submit it to the Collective Security Intelligence Cloud for a simple known-disposition lookup using the file's SHA-256 hash value. You can also submit files for *dynamic analysis*, which produces a threat score. Using this contextual information, you can configure the system to block or allow specific files.

You configure malware protection as part of your overall access control configuration; file policies associated with access control rules inspect network traffic that meets rule conditions.

FireAMP Integration

FireAMP is Cisco's enterprise-class, advanced malware analysis and protection solution that discovers, understands, and blocks advanced malware outbreaks, advanced persistent threats, and targeted attacks.

If your organization has a FireAMP subscription, individual users install *FireAMP Connectors* on their computers and mobile devices (also called *endpoints*). These lightweight agents communicate with the Collective Security Intelligence Cloud, which in turn communicates with the Defense Center.

After you configure the Defense Center to connect to the cloud, you can use the Defense Center web interface to view endpoint-based malware events generated as a result of scans, detections, and quarantines on the endpoints in your organization. The Defense Center also uses FireAMP data to generate and track indications of compromise on hosts, as well as display network file trajectories.

Use the *FireAMP portal* (http://amp.sourcefire.com/) to configure your FireAMP deployment. The portal helps you quickly identify and quarantine malware. You can identify outbreaks when they occur, track their trajectories, understand their effects, and learn how to successfully recover. You can also use FireAMP to create custom protections, block execution of certain applications based on group policy, and create custom whitelists.

Network File Trajectory

The network file trajectory feature allows you to track a file's transmission path across a network. The system uses SHA-256 hash values to track files; so, to track a file, the system must either:

- calculate the file's SHA-256 hash value and perform a malware cloud lookup using that value
- receive endpoint-based threat and quarantine data about that file, using the Defense Center's integration with your organization's FireAMP subscription

Each file has an associated trajectory map, which contains a visual display of the file's transfers over time as well as additional information about the file.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs). For detailed information, you can download additional documentation from the Support Site.

eStreamer

The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Cisco appliance to a custom-developed client application. After you create a client application, you can connect it to an eStreamer server (Defense Center or managed device), start the eStreamerservice, and begin exchanging data.

eStreamer integration requires custom programming, but allows you to request specific data from an appliance. If, for example, you display network host data within one of your network management applications, you could write a program to retrieve host criticality or vulnerability data from the Defense Center and add that information to your display.

External Database Access

The database access feature allows you to query several database tables on a Defense Center, using a third-party client that supports JDBC SSL connections.

You can use an industry-standard reporting tool such as Crystal Reports, Actuate BIRT, or JasperSoft iReport to design and submit queries. Or, you can configure your own custom application to query Cisco data. For example, you could build a servlet to report intrusion and discovery event data periodically or refresh an alert dashboard.

Host Input

The host input feature allows you to augment the information in the network map by importing data from third-party sources using scripts or command-line files.

The web interface also provides some host input functionality; you can modify operating system or application protocol identities, validate or invalidate vulnerabilities, and delete various items from the network map, including clients and server ports.

Remediation

The system includes an API that allows you to create remediations that your Defense Center can automatically launch when conditions on your network violate an associated correlation policy or compliance white list. This can not only automatically mitigate attacks when you are not immediately available to address them, but can also ensure that your system remains compliant with your organization's security policy. In addition to remediations that you create, the Defense Center ships with several predefined remediation modules.

Licensing Virtual Appliances

You can license a variety of features to create an optimal FireSIGHT System deployment for your organization. You must use the Defense Center to control licenses for itself and the devices it manages.

Cisco recommends you add the licenses your organization has purchased during the initial setup of your Defense Center. Otherwise, any devices you register during initial setup are added to the Defense Center as unlicensed. You must then enable licenses on each device individually after the initial setup process is over. For more information, see Setting Up Virtual Appliances, page 4-1.

A FireSIGHT license is included with each Defense Center purchase, and is required to perform host, application, and user discovery. The FireSIGHT license on a Defense Center also determines how many individual hosts and users you can monitor with the Defense Center and its managed devices, as well as how many users you can use to perform user control. For a virtual Defense Center, this limit is 50,000 individual hosts and users.

If your Defense Center was previously running Version 4.10.x, you may be able to use legacy RNA Host and RUA User licenses instead of a FireSIGHT license. For more information, see License Settings, page 4-10.

Additional model-specific licenses allow your managed devices to perform a variety of functions, as follows:

Protection

A Protection license allows virtual devices to perform intrusion detection and prevention, file control, and Security Intelligence filtering.

Control

A Control license allows virtual devices to perform user and application control. Although virtual devices do not support any of the hardware-based features granted to Series 2 and Series 3 devices by the Control license (such as switching or routing), virtual Defense Centers can manage those features on physical devices. A Control license requires a Protection license.

URL Filtering

A URL Filtering license allows virtual devices to use regularly updated cloud-based category and reputation data to determine which traffic can traverse your network, based on the URLs requested by monitored hosts. A URL Filtering license requires a Protection license.

Malware

A Malware license allows virtual devices to perform network-based advanced malware protection (AMP), that is, to detect and block malware in files transmitted over your network. It also allows you to view trajectories, which track files transmitted over your network. A Malware license requires a Protection license.

VPN

A VPN license allows you to use a virtual Defense Center to build secure VPN tunnels among the virtual routers on Series 3 devices, or from Series 3 devices to remote devices or other third-party VPN endpoints. A VPN license requires Protection and Control licenses.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. In general, you cannot license a capability that a device does not support; see Understanding Virtual Appliance Capabilities, page 1-3. The following table summarizes which licenses you can add to your virtual Defense Center and apply to each device model:

- The device rows indicate whether you can apply that license to the device using its managing Defense Center, including a Defense Center.
- The Defense Center rows (for all licenses except FireSIGHT) indicate whether that Defense Center can apply the license to devices (including virtual devices). For example, the DC500 cannot apply a URL Filtering license to a virtual device.

For example, you can use a virtual Defense Center to create a VPN deployment using Series 3 devices, but you cannot use a DC500 to perform category and reputation-based URL filtering, using virtual devices. Note that `n/a` marks Defense Center-based licenses that are not relevant to managed devices.

Table 1-4 Supported Licenses by Model

Models	FireSIGHT	Protection	Control	URL Filtering	Malware	VPN
Series 2 devices: • 3D500/1000/2000 • 3D2100/2500/3500/4500 • 3D6500 • 3D9900	n/a	automatic, no Security Intelligence	no	no	no	no
Series 3 devices: • 7000 Series • 8000 Series	n/a	yes	yes	yes	yes	yes
virtual devices	n/a	yes	yes, but no support for hardware features	yes	yes	no

Table 1-4 Supported Licenses by Model (continued)

Models	FireSIGHT	Protection	Control	URL Filtering	Malware	VPN
Sourcefire Software for X-Series	n/a	yes	yes, but no support for hardware features	yes	yes	no
Cisco ASA with FirePOWER Services	n/a	yes	yes, but no support for hardware features	yes	yes	no
DC500 Series 2 Defense Center	yes	yes, but no Security Intelligence	yes, but no user control	no	no	yes
DC1000/3000 Series 2 Defense Centers	yes	yes	yes	yes	yes	yes
DC750/1500/3500 Series 3 Defense Centers	yes	yes	yes	yes	yes	yes
virtual Defense Centers	yes	yes	yes	yes	yes	yes

For detailed information on licensing, see the Licensing the FireSIGHT System chapter in the *FireSIGHT System User Guide*.

Security, Internet Access, and Communication Ports

To safeguard the Defense Center, you must install the it 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 (or any managed devices) from outside the firewall.

If the Defense Center and its managed devices reside on the same network, you can connect the management interfaces on the devices to the same protected internal network as the Defense Center. This allows you to securely control the devices from the Defense Center.

Regardless of how you deploy your appliances, intra-appliance communication is encrypted. However, you must still take steps to ensure that communications between appliances cannot be interrupted, blocked, or tampered with; for example, with a distributed denial of service (DDoS) or man-in-the-middle attack.

Also note that specific features of the FireSIGHT System require an Internet connection. By default, all appliances are configured to directly connect to the Internet. Additionally, the system requires certain ports remain open for basic intra-appliance communication, for secure appliance access, and so that specific system features can access the local or Internet resources they need to operate correctly.

Tip With the exception of Sourcefire Software for X-Series and Cisco ASA with FirePOWER Services, FireSIGHT System appliances support the use of a proxy server. For more information, see the *FireSIGHT System User Guide*.

For more information, see:

- Internet Access Requirements, page 1-13

- Communication Ports Requirements, page 1-14

Internet Access Requirements

Virtual Defense Centers are configured to directly connect to the Internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP), which are open by default. On virtual devices, port 443 is open only if you enable a Malware license, so the device can submit files for dynamic analysis. For more information, see Communication Ports Requirements, page 1-14. FireSIGHT virtual appliances support use of a proxy server; for more information see the *FireSIGHT System User Guide*.

The following table describes the Internet access requirements of specific features of the FireSIGHT System.

Table 1-5 FireSIGHT System Feature Internet Access Requirements

Feature	Internet Access is Required to...	Appliances
dynamic analysis: querying	query the Collective Security Intelligence Cloud for threat scores of files previously submitted for dynamic analysis.	Defense Center
dynamic analysis: submitting	submit files to the Collective Security Intelligence Cloud for dynamic analysis.	Managed devices
FireAMP integration	receive endpoint-based (FireAMP) malware events from the Collective Security Intelligence Cloud.	Defense Center
intrusion rule, VDB, and GeoDB updates	download or schedule the download of a intrusion rule, GeoDB, or VDB update directly to an appliance.	Defense Center
network-based AMP	perform malware cloud lookups.	Defense Center
RSS feed dashboard widget	download RSS feed data from an external source, including Cisco.	Any except virtual devices, X-Series, and ASA FirePOWER
Security Intelligence filtering	download Security Intelligence feed data from an external source, including the FireSIGHT System Intelligence Feed.	Defense Center
system software updates	download or schedule the download of a system update directly to an appliance.	Any except virtual devices, X-Series, and ASA FirePOWER
URL filtering	download cloud-based URL category and reputation data for access control, and perform lookups for uncategorized URLs.	Defense Center
whois	request whois information for an external host.	Any except virtual devices, X-Series, and ASA FirePOWER

Communication Ports Requirements

FireSIGHT System appliances communicate using a two-way, SSL-encrypted communication channel, which by default uses port 8305/tcp. The system **requires** this port remain open for basic intra-appliance communication. Other open ports allow:

- access to an appliance's web interface
- secure remote connections to an appliance
- certain features of the system to access the local or Internet resources they need to function correctly

In general, feature-related ports remain closed until you enable or configure the associated feature. For example, until you connect the Defense Center to a User Agent, the agent communications port (3306/tcp) remains closed. As another example, port 623/udp remains closed on Series 3 appliances until you enable LOM.

Caution Do not close an open port until you understand how this action will affect your deployment.

For example, closing port 25/tcp (SMTP) outbound on a manage device blocks the device from sending email notifications for individual intrusion events (see the *FireSIGHT System User Guide*). As another example, you can disable access to a physical managed device's web interface by closing port 443/tcp (HTTPS), but this also prevents the device from submitting suspected malware files to the Collective Security Intelligence Cloud for dynamic analysis.

Note that the system allows you to change some of its communication ports:

- You can specify custom ports for LDAP and RADIUS authentication when you configure a connection between the system and the authentication server; see the *FireSIGHT System User Guide*.
- You can change the management port (8305/tcp); see the *FireSIGHT System User Guide*. However, Cisco **strongly** recommends that you keep the default setting. If you change the management port, you must change it for all appliances in your deployment that need to communicate with each other.
- You can use port 32137/tcp to allow upgraded Defense Centers to communicate with the Collective Security Intelligence Cloud. However, Cisco recommends you switch to port 443, which is the default for fresh installations of Version 5.3 and later. For more information, see the *FireSIGHT System User Guide*.

The following table lists the open ports required by each appliance type so that you can take full advantage of FireSIGHT System features.

Table 1-6 Default Communication Ports for FireSIGHT System Features and Operations

Port	Description	Direction	Is Open on...	To...
22/tcp	SSH/SSL	Bidirectional	Any	allow a secure remote connection to the appliance.
25/tcp	SMTP	Outbound	Any	send email notices and alerts from the appliance.
53/tcp	DNS	Outbound	Any	use DNS.
67/udp 68/udp	DHCP	Outbound	Any except X-Series	use DHCP. **Note** These ports are **closed** by default.

Table 1-6 Default Communication Ports for FireSIGHT System Features and Operations (continued)

Port	Description	Direction	Is Open on...	To...
80/tcp	HTTP	Outbound	Any except virtual devices, X-Series, and ASA FirePOWER	allow the RSS Feed dashboard widget to connect to a remote web server.
		Bidirectional	Defense Center	update custom and third-party Security Intelligence feeds via HTTP. download URL category and reputation data (port 443 also required).
161/udp	SNMP	Bidirectional	Any except X-Series and ASA FirePOWER	allow access to an appliance's MIBs via SNMP polling.
162/udp	SNMP	Outbound	Any	send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	Outbound	Any except virtual devices and X-Series	communicate with an LDAP server for external authentication.
389/tcp 636/tcp	LDAP	Outbound	Defense Center	obtain metadata for detected LDAP users.
443/tcp	HTTPS	Inbound	Any except virtual devices, X-Series, and ASA FirePOWER	access the appliance's web interface.
443/tcp	HTTPS AMQP cloud comms.	Bidirectional	Defense Center	obtain: • software, intrusion rule, VDB, and GeoDB updates • URL category and reputation data (port 80 also required) • the Collective Security Intelligence feed and other secure Security Intelligence feeds • endpoint-based (FireAMP) malware events • malware dispositions for files detected in network traffic • dynamic analysis information on submitted files
			Series 2 and Series 3 devices	download software updates using the device's local web interface.
			Series 3, virtual devices, X-Series, and ASA FirePOWER	submit files to for dynamic analysis.
514/udp	syslog	Outbound	Any	send alerts to a remote syslog server.
623/udp	SOL/LOM	Bidirectional	Series 3	allow you to perform Lights-Out Management using a Serial Over LAN (SOL) connection.

Table 1-6 Default Communication Ports for FireSIGHT System Features and Operations (continued)

Port	Description	Direction	Is Open on...	To...
1500/tcp 2000/tcp	Inbound	TCP	Defense Center	allow read-only access to the database by a third-party client.
1812/udp 1813/udp	RADIUS	Bidirectional	Any except virtual devices, X-Series, and ASA FirePOWER	communicate with a RADIUS server for external authentication and accounting.
3306/tcp	User Agent	Inbound	Defense Center	communicate with User Agents.
8302/tcp	eStreamer	Bidirectional	Any except virtual devices and X-Series	communicate with an eStreamer client.
8305/tcp	device management	Bidirectional	Any	securely communicate between appliances in a deployment. **Required**.
8307/tcp	host input client	Bidirectional	Defense Center	communicate with a host input client.
32137/tcp	cloud comms.	Bidirectional	Defense Center	allow upgraded Defense Centers to communicate with the Collective Security Intelligence Cloud cloud.

CHAPTER 2

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.

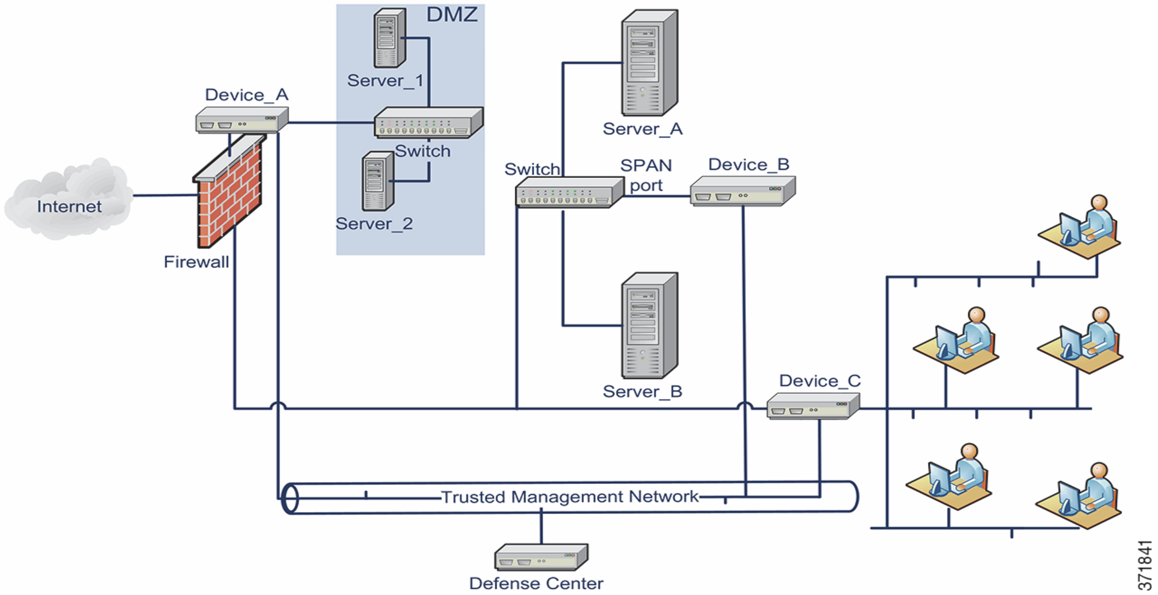
⚠ **Caution** Cisco **strongly** recommends that you keep your production network traffic and your trusted management network traffic on different network segments. You must take precautions to ensure the security of the appliances and the management traffic data stream.

This chapter provides deployment examples for:

- Typical FireSIGHT System Deployment, page 2-1
- VMware Virtual Appliance Deployments, page 2-2

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:

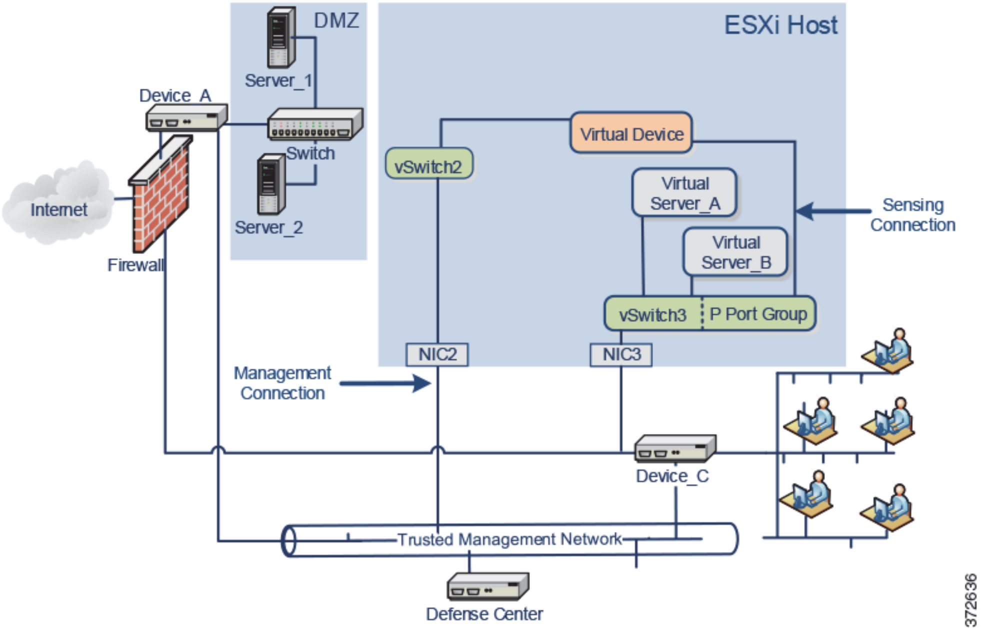
- Adding Virtualization and a Virtual Device, page 2-2
- Using the Virtual Device for Inline Detection, page 2-3
- Adding a Virtual Defense Center, page 2-4
- Using a Remote Office Deployment, page 2-5

Adding Virtualization and a Virtual Device

You can replace the physical internal servers in our Typical FireSIGHT System Deployment, page 2-1 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.



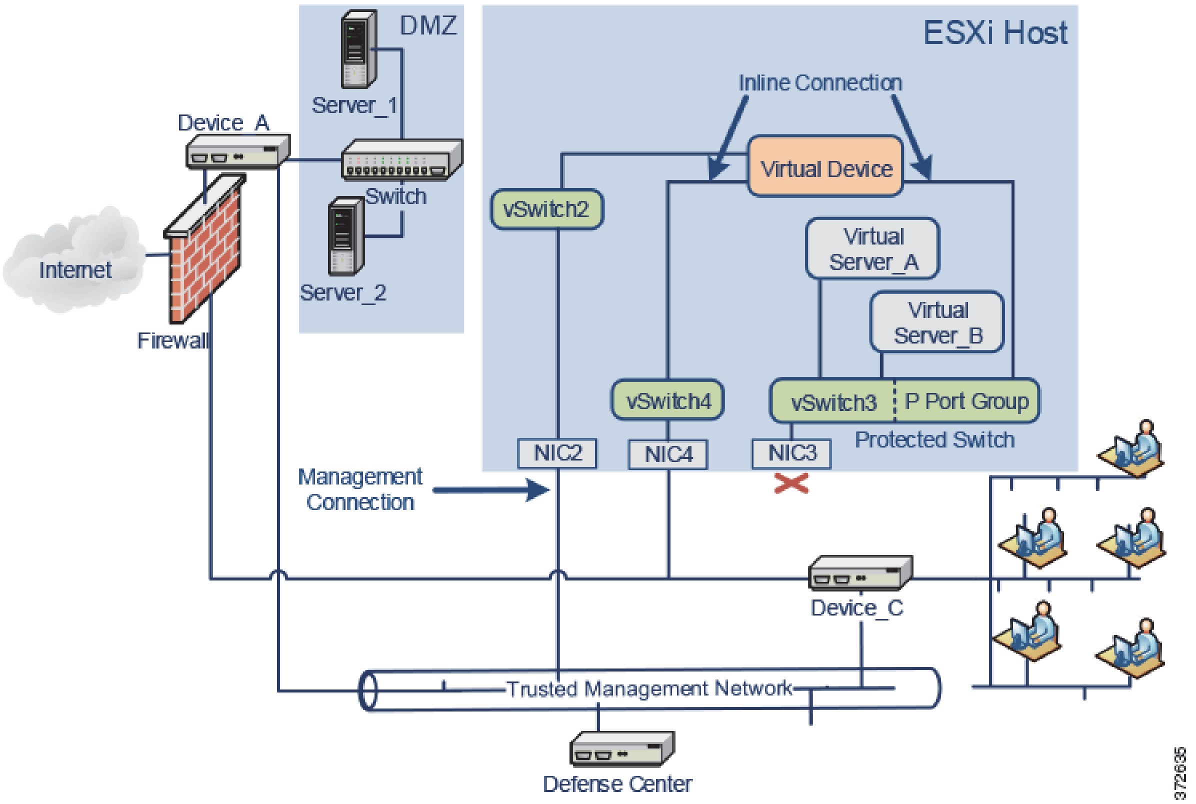
Note To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See Configuring Virtual Device Interfaces, page 3-9.

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 2-1 and on the example shown in Adding Virtualization and a Virtual Device, page 2-2.

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 Interfaces, page 3-9.

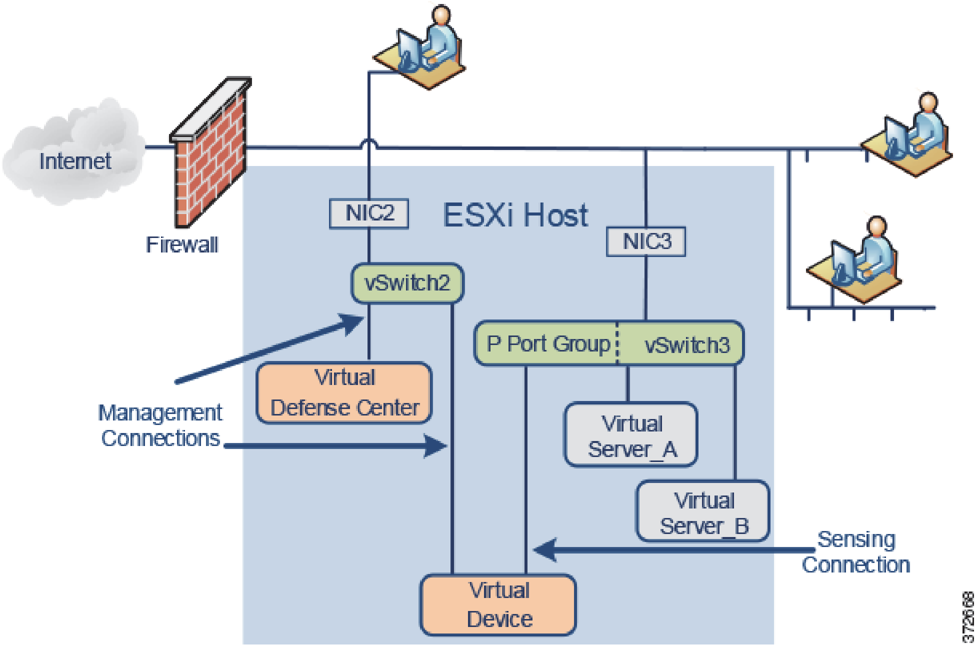
The virtual device monitors and drops any malicious traffic to Server_A and Server_B, depending on your intrusion policy.

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 2-1 and on the example shown in Using the Virtual Device for Inline Detection, page 2-3.

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.

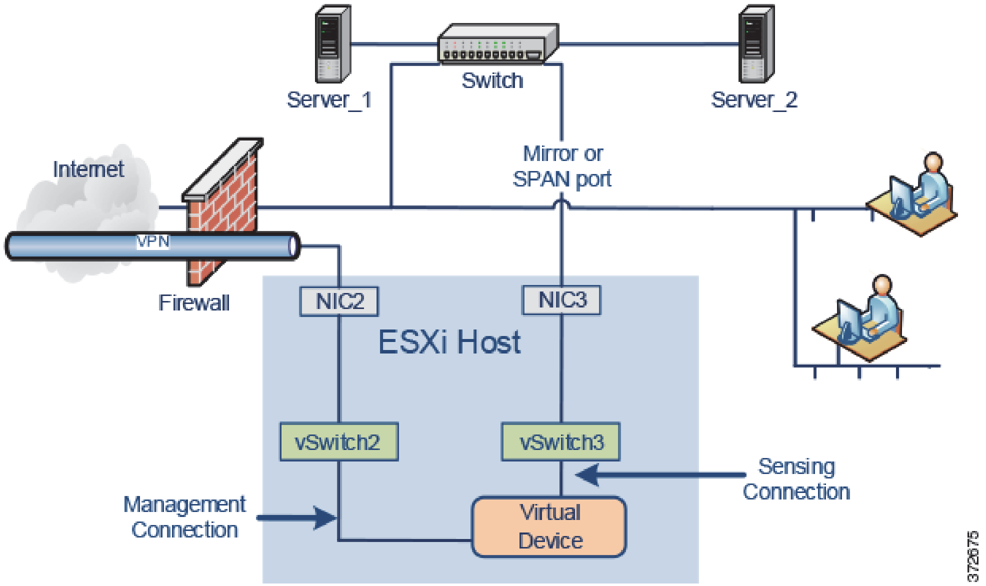


Your sensing connection on your virtual device must be allowed to monitor network traffic. The virtual switch, or the port group on that switch to which the virtual interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In the example, the P Port Group is set to accept promiscuous mode traffic. See Configuring Virtual Device Interfaces, page 3-9.

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 4-7 and Setting Up a Virtual Device Using the CLI, page 4-3 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 Interfaces, page 3-9.

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 4-3 for information on setting up the virtual device management connections.

Installing Virtual Appliances

Cisco provides packaged virtual appliances for VMware ESXi host environments on its Support Site as compressed archive (`.tar.gz`) files. Cisco virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware.

You deploy a virtual appliance with a virtual infrastructure (VI) or ESXi Open Virtual Format (OVF) template:

- When you deploy with a VI OVF template, you can configure FireSIGHT System-required settings (such as the password for the admin account and settings that allow the appliance to communicate on your network) using the setup wizard in the deployment.
- You must deploy to a managing platform, either VMware vCloud Director or VMware vCenter.
- When you deploy with an ESXi OVF template, you must configure settings after installation using the command line interface (CLI) on the VMware console of the virtual appliance.
- You can deploy to a managing platform (VMware vCloud Director or VMware vCenter), or you can deploy as a standalone appliance.

Note VMware snapshots of Cisco virtual appliances are **not** supported.

Use the instructions in this chapter to download, install, and configure a Cisco virtual appliance. For help creating a virtual host environment, see the VMware ESXi documentation.

After you install and configure a virtual appliance according to the following procedures, power it on to initialize it and begin the initial setup process as described in the next chapter. For information on uninstalling a virtual appliance, see Uninstalling a Virtual Appliance, page 3-10.

To install and deploy a Cisco virtual appliance:

Step 1 Make sure your planned deployment meets the prerequisites described in Operating Environment Prerequisites, page 1-5.

Step 2 Obtain the correct archive files from the Support Site, copy them to an appropriate storage medium, and decompress them; see Obtaining the Installation Files, page 3-2.

Step 3 Use the VMware vCloud Director web portal or vSphere Client to install the virtual appliance, but do not power it on; see Installing a Virtual Appliance, page 3-3.

Step 4 Confirm and adjust network, hardware, and memory settings; see Updating Important Settings Post-Installation, page 3-8.

Step 5 Make sure the sensing interfaces on virtual devices are correctly connected to an ESXi host virtual switch; see Configuring Virtual Device Interfaces, page 3-9.

Obtaining the Installation Files

Cisco provides compressed archive (`.tar.gz`) files for installing virtual appliances: one for Defense Centers and one for devices. Each archive contains the following files:

- an Open Virtual Format (`.ovf`) template containing `-ESXi-` in the file name
- an Open Virtual Format (`.ovf`) template containing `-VI-` in the file name
- a Manifest File (`.mf`) containing `-ESXi-` in the file name
- a Manifest File (`.mf`) containing `-VI-` in the file name
- the Virtual Machine Disk Format (`.vmdk`)

Before you install a virtual appliance, obtain the correct archive file from the Support Site. Cisco recommends that you always use the most recent package available. Virtual appliance packages are usually associated with major versions of the system software (for example, 5.2 or 5.3).

To obtain virtual appliance archive files:

Step 1 Using the user name and password for your support account, log into the Support Site (https://support.sourcefire.com/).

Step 2 Click **Downloads**, select the **3D System** tab on the page that appears, and then click the major version of the system software you want to install.

For example, to download a Version 5.3.1 archive file, click **Downloads > 3D System > 5.3**.

Step 3 Find the archive file that you want to download for either the virtual device or virtual Defense Center, using the following naming convention:

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx.tar.gz
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx.tar.gz
```

where *`X.X.X-xxx`* is the version and build number of the archive file you want to download.

You can click one of the links on the left side of the page to view the appropriate section of the page. For example, click **5.3 Virtual Appliances** to view the archive files for Version 5.3.1 of the FireSIGHT System.

Step 4 Click the archive you want to download.

The file begins downloading.

Tip While you are logged into the Support Site, Cisco recommends you download any available updates for virtual appliances so that after you install a virtual appliance to a major version, you can update its system software. You should always run the latest version of the system software supported by your appliance. For Defense Centers, you should also download any new intrusion rule and Vulnerability Database (VDB) updates.

Step 5 Copy the archive file to a location accessible to the workstation or server that is running the vSphere Client or VMware vCloud Director web portal.

Caution Do **not** transfer archive files via email; the files can become corrupted.

Step 6 Decompress the archive file using your preferred tool and extract the installation files.

For the virtual device:

```
Sourcefire_3D_Device_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.mf
```

For the virtual Defense Center:

```
Sourcefire_Defense_Center_Virtual64_VMware-X.X.X-xxx-disk1.vmdk
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.mf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.mf
```

where *X.X.X-xxx* is the version and build number of the archive file you downloaded.

Make sure you keep all the files in the same directory.

Step 7 Continue with Installing a Virtual Appliance to deploy the virtual appliance.

Installing a Virtual Appliance

To install a virtual appliance, you deploy an OVF (VI or ESXi) template to a managing platform (VMware vCloud Director or VMware vCenter) using a platform interface (VMware vCloud Director web portal or vSphere Client):

- If you deploy using a VI OVF template, you can configure FireSIGHT System-required settings during installation. You must manage this virtual appliance using either VMware vCloud Director or VMware vCenter.
- If you deploy using an ESXi OVF template, you must configure FireSIGHT System-required settings after installation. You can manage this virtual appliance using either VMware vCloud Director or VMware vCenter, or use it as a standalone appliance.

After you make sure your planned deployment meets the prerequisites (described in Operating Environment Prerequisites, page 1-5) and download the necessary archive files, use the VMware vCloud Director web portal or vSphere Client to install virtual appliances.

You have the following installation options for installing a virtual appliance:

- For a virtual Defense Center:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- For the virtual device:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

where *X.X.X-xxx* is the version and build number of the file you want to use.

The following table lists the information required for deployment:

Table 3-1 VMware OVF Template

Setting	Action
Import/Deploy OVF Template	Browse to the OVF templates you downloaded in the previous procedure to use.
OVF Template Details	Confirm the appliance you are installing (virtual Defense Center or virtual device) and the deployment option (`VI` or `ESXi`).
Name and Location	Enter a unique, meaningful name for your virtual appliance and select the inventory location for your appliance.
Host / Cluster	For virtual devices only, select the host or cluster where you want to deploy the device.
Disk Format	Select the format to store the virtual disks: thick provision lazy zeroed, thick provision eager zeroed, or thin provision.
Network Mapping	Select the management interface for the virtual appliance.

If you deploy with a VI OVF template, the installation process allows you to perform basic setup for virtual Defense Centers and the entire initial setup for virtual devices. You can specify:

- a new password for the admin account
- network settings that allow the appliance to communicate on your management network
- for virtual devices only, the initial detection mode
- for virtual devices only, the managing Defense Center

If you deploy with an ESXi OVF template or if you choose not to configure with the setup wizard, you must perform the initial setup for virtual appliances using the VMware console. For detailed information on performing the initial setup, including guidance on what configurations to specify, see Setting Up Virtual Appliances, page 4-1.

Use one of the following options to install your virtual appliance:

- Installing with the VMware vCloud Director Web Portal, page 3-4 describes how to deploy a virtual appliance to the VMware vCloud Director.
- Installing with vSphere Client, page 3-6 describes how to deploy a virtual appliance to the VMware vCenter.

To understand network settings and detection modes, see Setting Up a Virtual Device Using the CLI, page 4-3 and Setting Up a Virtual Defense Center, page 4-6.

Installing with the VMware vCloud Director Web Portal

You can use VMware vCloud Director web portal to deploy a virtual appliance using the following steps:

- Create an organization and catalog to contain the vApp templates. For more information, see the *VMware vCloud Director User's Guide*.
- Upload the FireSIGHT System virtual appliance OVF packages to the catalog as vApp templates. For more information, see Uploading the Virtual Appliance OVF Packages, page 3-5.
- Create a virtual appliance using a vApp template. For more information, see Using the vApp Template, page 3-5.

Uploading the Virtual Appliance OVF Packages

You can upload the following OVF packages the following OVF packages to your VMware vCloud Director organization catalog:

- For the virtual Defense Center:

  Sourcefire_Defense_Center_Virtual64_VMware-VI-*X.X.X*-   *xxx*.ovf

- For the virtual device:

  Sourcefire_3D_Device_Virtual64_VMware-VI-*X.X.X-xxx*.ovf

where *X.X.X-xxx* is the version and build number of the OVF package you want to upload.

To upload the virtual appliance OVF packages:

Step 1 On the VMware vCloud Director web portal, select **Catalogs >** *Organization* **> vApp Templates** where *Organization* is the name of the organization that you want to contain your vApp templates.

Step 2 On the vApp Templates media tab, click the Upload icon (⬆).

The Upload OVF package as a vApp Template pop-up window appears.

Step 3 In the OVF package field, enter the location of the OVF package, or click **Browse** to browse to the OVF package:

- For the virtual Defense Center:

  Sourcefire_Defense_Center_Virtual64_VMware-VI-*X.X.X-xxx*.ovf

- For the virtual device:

  Sourcefire_3D_Device_Virtual64_VMware-VI-*X.X.X-xxx*.ovf

- where *X.X.X-xxx* is the version and build number of the OVF package you want to upload.

Step 4 Enter a name and optionally a description for the OVF package.

Step 5 From the drop-down lists, select the virtual datacenter, storage profile, and catalog to contain the vApp template.

Step 6 Click **Upload** to upload the OVF package as a vApp template to the catalog.

The OVF package uploads to your organization's catalog.

Step 7 Continue with Using the vApp Template to create a virtual appliance from the vApp template.

Using the vApp Template

You can use a vApp template to create a virtual appliance allows you to configure FireSIGHT System-required settings during the installation using a setup wizard. After you specify settings on each page of the wizard, click **Next** to continue. For your convenience, the final page of the wizard allows you to confirm your settings before completing the procedure.

To use the vApp template to create a virtual appliance:

Step 1 On the VMware vCloud Director web portal, select **My Cloud > vApps**.

Step 2 On the vApps media tab, click the Add icon (✚) to add a vApp from the catalog.

The Add vApp from Catalog pop-up window appears.

Step 3 Click **All Templates** on the template menu bar.

A list of all available vApp templates is displayed.

Step 4 Select the vApp template you want to add to display a description of the virtual appliance.

- For the virtual Defense Center:

  `Sourcefire_Defense_Center_Virtual64_VMware-VI-`*`X.X.X-xxx`*`.ovf`

- For the virtual device:

  `Sourcefire_3D_Device_Virtual64_VMware-VI-`*`X.X.X-xxx`*`.ovf`

  where *`X.X.X-xxx`* is the version and build number of the archive file.

The End User License Agreement (EULA) appears.

Step 5 Read and accept the EULA.

The Name this vApp screen appears.

Step 6 Enter a name and optionally a description for the vApp.

The Configure Resources screen appears.

Step 7 On the Configure Resources screen, select the virtual datacenter, enter a computer name (or using the default computer name), and select the storage profile.

The Network Mapping screen appears.

Step 8 Map the networks used in the OVF template to a network in your inventory by selecting the destination for the external, management, and internal sources, and your IP allocation.

The Custom Properties screen appears.

Step 9 Optionally, on the Custom Properties screen, perform the initial setup for the appliance by entering the FireSIGHT System-required settings on the setup wizard. If you do not perform the initial setup now, you can do it later using the instructions in Setting Up Virtual Appliances, page 4-1.

The Ready to Complete screen appears, which displays the configuration for your virtual appliance.

Step 10 Confirm your settings and click **Finish**.

Note Do **not** enable the **Power on after deployment** option for a virtual device. You must map your sensing interfaces and be sure they are set to connect before powering on the appliance. For more information, see Initializing a Virtual Appliance, page 4-2.

Step 11 Continue with Updating Important Settings Post-Installation, page 3-8.

Installing with vSphere Client

You can use the vSphere Client to deploy with either a VI OVF or ESXi OVF template:

- If you deploy using a VI OVF template, the appliance must be managed by VMware vCenter or VMware vCloud Director.
- If you deploy using a ESXi OVF template, the appliance can be managed by VMware vCenter, VMware vCloud Director, or deployed to a standalone host. In either case, you must configure FireSIGHT System-required settings after installation.

After you specify settings on each page of the wizard, click **Next** to continue. For your convenience, the final page of the wizard allows you to confirm your settings before completing the procedure.

To install a virtual appliance using vSphere Client:

Step 1 Using the vSphere Client, deploy the OVF template file you downloaded earlier by clicking **File > Deploy OVF Template**.

The Source screen appears, where you can browse through a drop-down list for the template you want to deploy.

Step 2 From the drop-down list, select the OVF template you want to deploy:

- For the virtual Defense Center:

```
Sourcefire_Defense_Center_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_Defense_Center_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

- For the virtual device:

```
Sourcefire_3D_Device_Virtual64_VMware-VI-X.X.X-xxx.ovf
Sourcefire_3D_Device_Virtual64_VMware-ESXi-X.X.X-xxx.ovf
```

where `X.X.X-xxx` is the version and build number of the archive file you downloaded.

The OVF Template Details screen appears.

Step 3 Confirm that you selected the correct virtual machine:

- For the ESXi OVF template:

  The Name and Location screen appears.

- For the VI OVF template:

  The End User License Agreement (EULA) screen appears.

  Read and accept the EULA, then the Name and Location screen appears.

Step 4 Type the name for your virtual appliance in the text field, and select the inventory location for where you want to deploy the appliance.

The Host / Cluster screen appears.

Step 5 Select the host or cluster where you want to deploy the template.

The Specific Host screen appears.

Step 6 Select the specific host within the cluster where you want to deploy the template.

The Storage screen appears.

Step 7 Select the destination storage for the virtual machine.

The Disk Format screen appears.

Step 8 Select which format you want to store the virtual disks from the following options:

- thick provision lazy zeroed
- thin provision eager zeroed
- thin provision

The Network Mapping screen appears.

Step 9 Select the network where you want to deploy the template:

- For the ESXi OVF template:

  The ESXi Finish screen appears.

- For the VI OVF template:

  The Properties screen appears.

  Enter the FireSIGHT System-required settings for the appliance or click through to complete the setup later, confirm your settings, then click **Finish**.

Note Do **not** enable the **Power on after deployment** option for a virtual device. You must map your sensing interfaces and be sure they are set to connect before powering on the appliance. For more information, see Initializing a Virtual Appliance, page 4-2.

Step 10 After the installation is complete, close the status window.

Step 11 Continue with Updating Important Settings Post-Installation.

Updating Important Settings Post-Installation

After you install a virtual appliance, you must confirm that the virtual appliance's hardware and memory settings meet the requirements for your deployment. Do **not** decrease the default settings, as they are the minimum required to run the system software. However, to improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. The following table lists the default appliance settings.

Table 3-2 Default Virtual Appliance Settings

Setting	Default	Adjustable Setting?
memory	4GB	yes, and for a virtual device you **must** allocate: • 4GB minimum • 5GB to add category and reputation-based URL filtering • 6GB to add Security Intelligence filtering using large dynamic feeds • 7GB to add URL filtering and Security Intelligence
virtual CPUs	4	yes, up to 8
hard disk provisioned size	40GB (device) 250GB (Defense Center)	no

The following procedure explains how to check and adjust a virtual appliance's hardware and memory settings.

To check your virtual appliance settings:

Step 1 Right-click the name of your new virtual appliance, then select **Edit Settings** from the context menu, or click **Edit virtual machine settings** from the **Getting Started** tab in the main window.

The Virtual Machine Properties pop-up window appears, displaying the Hardware tab.

Step 2 Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set no lower than the defaults, as described in Table 3-2Default Virtual Appliance Settings, page 3-8.

The memory setting and the number of virtual CPUs for the appliance are listed on the left side of the window. To see the hard disk **Provisioned Size**, click **Hard disk 1**.

Step 3 Optionally, increase the memory and number of virtual CPUs by clicking the appropriate setting on the left side of the window, then making changes on the right side of the window.

Step 4 Confirm the **Network adapter 1** settings are as follows, making changes if necessary:

- Under **Device Status**, enable the **Connect at power on** check box.
- Under **MAC Address**, manually set the MAC address for your virtual appliance’s management interface.
- Manually assign the MAC address to your virtual device to avoid MAC address changes or conflicts from other systems in the dynamic pool.
- Additionally, for virtual Defense Centers, setting its MAC address manually ensures that you will not have to re-request licenses from Cisco if you ever have to reimage the appliance.
- Under **Network Connection**, set the **Network label** to the name of the management network for your virtual appliance.

Step 5 Click **OK**.

Your changes are saved.

Step 6 The next step depends on the type of appliance you just installed:

- A virtual Defense Center is ready to initialize: continue with Setting Up Virtual Appliances, page 4-1.
- A virtual device needs some additional configurations: continue with Configuring Virtual Device Interfaces.

Configuring Virtual Device Interfaces

The interfaces on a virtual device must have a network connection to a port on an ESXi host virtual switch that accepts promiscuous mode.

Tip Add a port group to a virtual switch to isolate promiscuous mode virtual network connections from your production traffic. For information on adding port groups and setting security attributes, see your VMware documentation.

To permit promiscuous mode:

Step 1 Use the vSphere Client to log into your server and click on your server’s **Configuration** tab.

The **Hardware** and **Software** selection lists appear.

Step 2 In the **Hardware** list, click **Networking**.

The virtual switch diagram appears.

Step 3 On the switch and port group where you connect the sensing interfaces of the virtual device, click **Properties**.

The **Switch Properties** pop-up window appears.

Step 4 On the **Switch Properties** pop-up window, click **Edit**.

The **Detailed Properties** pop-up window appears.

Step 5 On the **Detailed Properties** pop-up window, select the **Security** tab.

Under **Policy Exceptions > Promiscuous Mode**, confirm that the Promiscuous Mode is set to **Accept**.

Tip To monitor VLAN traffic in your virtual environment, set the VLAN ID of the promiscuous port to 4095.

Step 6 Save your changes.

The device is ready to initialize.

Step 7 Continue with the next chapter, Setting Up Virtual Appliances, page 4-1.

Uninstalling a Virtual Appliance

You may need to uninstall or remove your virtual appliances. Shut down the virtual appliance, then uninstall a virtual appliance by deleting it.

Tip After you remove the virtual device, remember to return the sensing connections virtual switch port group to the default setting: **Promiscuous Mode**: **Reject**. For more information, see Configuring Virtual Device Interfaces, page 3-9.

Shutting Down a Virtual Appliance

Use the following procedure to properly shut down a virtual appliance.

To shut down a virtual appliance:

Step 1 At the VMware console, log in as a user with Administrator (or, for virtual devices, CLI Configuration) privileges. If you are using a virtual device, type `expert` to display the shell prompt.

The prompt for the appliance appears.

Step 2 Shut down the virtual appliance:

- On a virtual Defense Center, type `sudo shutdown -h now`.
- On a virtual device, type `system shutdown`.

The virtual appliance shuts down.

Deleting a Virtual Appliance

After the virtual appliance powers off, you can delete the virtual appliance.

Use the following procedure to delete a virtual appliance deployed on VMware vCloud Director:

To delete the virtual appliance using VMware vCloud Director web portal:

Step 1 Select **My Cloud > vApps**, right-click on the vApp you want to delete and click **Delete** from the menu, then click **Yes** on the confirmation pop-up window.

The virtual appliance is uninstalled.

Use the following procedure to delete a virtual appliance deployed on VMware vCenter:

To delete a virtual appliance using the vSphere Client:

Step 1 Click on name of the appliance in the vSphere Client context menu and click **Delete** using the Inventory menu, then click **Yes** in the confirmation dialog box.

The virtual appliance is uninstalled.

Setting Up Virtual Appliances

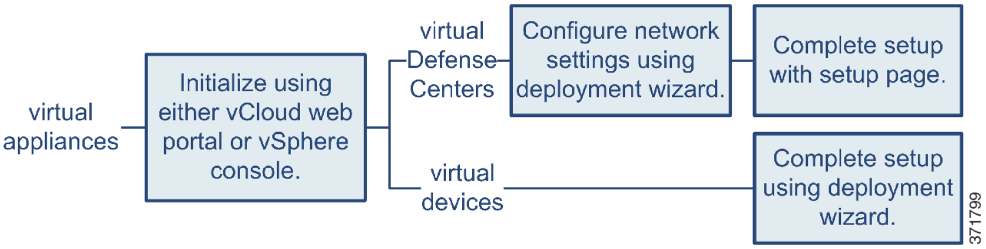
After you install a virtual appliance, you must complete a setup process that allows the new appliance to communicate on your trusted management network. You must also change the administrator password and accept the end user license agreement (EULA).

The setup process also allows you to perform many initial administrative-level tasks, such as setting the time, registering and licensing devices, and scheduling updates. The options you choose during setup and registration determine the default interfaces, inline sets, zones, and policies that the system creates and applies.

The purpose of these initial configurations and policies is to provide an out-of-the-box experience and to help you quickly set up your deployment, not to restrict your options. Regardless of how you initially configure a device, you can change its configuration at any time using the Defense Center. In other words, choosing a detection mode or access control policy during setup, for example, does not lock you into a specific device, zone, or policy configuration.

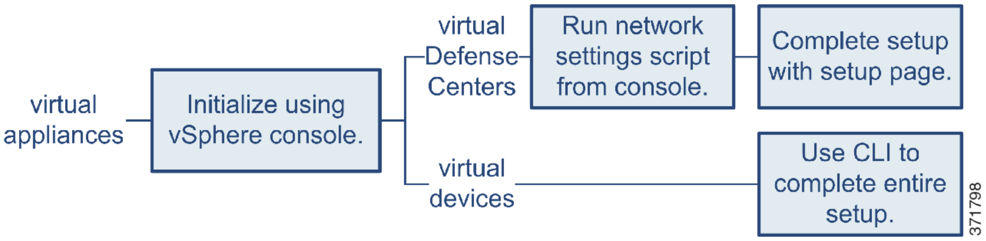
VI OVF Template Deployment

The following diagram shows the general process of setting up virtual Defense Centers and managed devices when you deploy with a VI OVF template.


virtual appliances
Initialize using either vCloud web portal or vSphere console.
virtual Defense Centers
Configure network settings using deployment wizard.
Complete setup with setup page.
virtual devices
Complete setup using deployment wizard.
371799

ESXi OVF Template Deployment

The following diagram shows the general process of setting up virtual Defense Centers and managed devices when you deploy with a ESXi OVF template.


virtual appliances
Initialize using vSphere console.
virtual Defense Centers
Run network settings script from console.
Complete setup with setup page.
virtual devices
Use CLI to complete entire setup.
371798

Regardless of how you deploy, begin by powering on the appliance to initialize it. After initialization completes, log in using the VMware console and complete the setup in one of the following ways, depending on the appliance type:

Virtual Devices

Virtual devices to not have a web interface. If you deploy with the VI OVF template, you can perform the device's initial setup, including registering it to a Defense Center, using the deployment wizard. If you deploy with the ESXi OVF template, you must use the interactive command line interface (CLI) to perform the initial setup.

Virtual Defense Centers

If you deploy with the VI OVF template, you can perform the network configuration using the wizard in the deployment. If you choose not to use the setup wizard or you deploy with the ESXi OVF template, configure network settings using a script. After your network is configured, complete the setup process using a computer on your management network to browse to the Defense Center's web interface.

Tip If you are deploying multiple appliances, set up your devices first, then their managing Defense Center. The initial setup process for a device allows you to preregister it to a Defense Center; the setup process for a Defense Center allows you to add and license preregistered managed devices.

For more information, see:

- Initializing a Virtual Appliance, page 4-2
- Setting Up a Virtual Device Using the CLI, page 4-3
- Setting Up a Virtual Defense Center, page 4-6
- Next Steps, page 4-12

Initializing a Virtual Appliance

After you install a virtual appliance, initialization starts automatically when you power on the virtual appliance for the first time.

Caution Startup time depends on a number of factors, including server resource availability. It can take up to 40 minutes for the initialization to complete. Do **not** interrupt the initialization or you may have to delete the appliance and begin again.

Use the following procedure to initialize a virtual appliance.

To initialize a virtual appliance:

Step 1 Power on the appliance:

- In the VMware vCloud Director web portal, select the vApp from the display, then click **Start**.
- In the vSphere Client, right-click the name of your imported virtual appliance from the inventory list, then select **Power > Power On** from the context menu.

Step 2 Monitor the initialization on the VMware console tab.

Messages appear during the two lengthiest portions of the process. After the process concludes, a login prompt appears.

Your next step depends on the appliance type and deployment.

If you used a VI OVF template and configured your FireSIGHT System-required settings during deployment:

- For the virtual Defense Center, continue with Setting Up a Virtual Defense Center, page 4-6 to complete the setup.
- For the virtual device, no further configuration is required.

If you used an ESXi OVF template or you did not configure FireSIGHT System-required settings when you deployed with the VI OVF template:

- For the virtual Defense Center, continue with Setting Up a Virtual Defense Center, page 4-6 to set up a virtual Defense Center by configuring its network settings using a script.
- For the virtual device, continue with Setting Up a Virtual Device Using the CLI, page 4-3 to set up a virtual device using the CLI.

Setting Up a Virtual Device Using the CLI

Because virtual devices do not have web interfaces, you must set up a virtual device using the CLI if you deployed with an ESXi OVF template. You can also use the CLI to configure FireSIGHT System-required settings if you deployed with a VI OVF template and did not use the setup wizard during deployment.

Tip If you deployed with a VI OVF template and used the setup wizard, your virtual device is configured and no further action is required.

When you first log into a newly configured device, you must read and accept the EULA. Then, follow the setup prompts to change the administrator password, and configure the device's network settings and detection mode.

When following the setup prompts, for multiple-choice questions, your options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

Note that the CLI prompts you for much of the same setup information that a physical device's setup web page does. For more information, see the *FireSIGHT System Installation Guide*.

Tip To change any of these settings for a virtual device after you complete the initial setup, you must use the CLI. For more information, see the Command Line Reference chapter in the *FireSIGHT System User Guide*.

Understanding Device Network Settings

The FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway. You can also specify up to three DNS servers, as well as the host name and domain for the device. Note that the host name is not reflected in the syslog until after you reboot the device.

Understanding Detection Modes

The detection mode you choose for a virtual device determines how the system initially configures the device's interfaces, and whether those interfaces belong to an inline set or security zone. The detection mode is not a setting you can change later; it is simply an option you choose during setup that helps the system tailor the device's initial configurations. In general, you should choose a detection mode based on how your device is deployed.

Passive

Choose this mode if your device is deployed passively, as an intrusion detection system (IDS). In a passive deployment, virtual devices can perform network-based file and malware detection, and Security Intelligence monitoring, as well as network discovery.

Inline

Choose this mode if your device is deployed inline, as an intrusion prevention system (IPS).

Note Although general practice in IPS deployments is to fail open and allow non-matching traffic, inline sets on virtual devices lack bypass capability.

Network Discovery

Choose this mode if your device is deployed passively, to perform host, application, and user discovery only.

The following table lists the interfaces, inline sets, and zones that the system creates depending on the detection mode you choose.

Table 4-1 Initial Configurations Based on Detection Mode

Detection Mode	Security Zones	Inline Sets	Interfaces
Inline	Internal and External	Default Inline Set	first pair added to Default Inline Set—one to the Internal and one to the External zone
Passive	Passive	none	first pair assigned to Passive zone
Network Discovery	Passive	none	first pair assigned to Passive zone

Note that security zones are a Defense Center-level configuration which the system does not create until you actually add the device to the Defense Center. At that time, if the appropriate zone (Internal, External, or Passive) already exists on the Defense Center, the system adds the listed interfaces to the existing zone. If the zone does not exist, the system creates it and adds the interfaces. For detailed information on interfaces, inline sets, and security zones, see the *FireSIGHT System User Guide*.

To set up a virtual device using its CLI:

Access: Admin

Step 1 Log into the virtual device at the VMware console using `admin` as the username and the new admin account password that you specified in the deployment setup wizard.

If you did not change the password using the wizard or you are deploying with a ESXi OVF template, use `Cisco` as the password.

The device immediately prompts you to read the EULA.

Step 2 Read and accept the EULA.

Step 3 Change the password for the `admin` account. This account has the Configuration CLI access level, and cannot be deleted.

Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Step 4 Configure network settings for the device.

First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

- enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of `255.255.0.0`.
- enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of `112`.

The VMware console may display messages as your settings are implemented.

Step 5 Specify the detection mode based on how you deployed the device.

The VMware console may display messages as your settings are implemented. When finished, the device reminds you to register this device to a Defense Center, and displays the CLI prompt.

Step 6 To use the CLI to register the device to the Defense Center that will manage it, continue with the next section, Registering a Virtual Device to a Defense Center, page 4-5.

You must manage devices with a Defense Center. If you do not register the device now, you must log in later and register it before you can add it to a Defense Center.

Registering a Virtual Device to a Defense Center

Because virtual devices do not have web interfaces, you must use the CLI to register a virtual device to a Defense Center, which can be physical or virtual. It is easiest to register a device to its Defense Center during the initial setup process, because you are already logged into the device's CLI.

To register a device, use the `configure manager add` command. A unique self-generated alphanumeric registration key is always required to register a device to a Defense Center. This is a simple key that you specify, and is not the same as a license key.

In most cases, you must provide the Defense Center's IP address along with the registration key, for example:

```
configure manager add XXX.XXX.XXX.XXX my_reg_key
```

where *`XXX.XXX.XXX.XXX`* is the IP address of the managing Defense Center and *`my_reg_key`* is the registration key you entered for the virtual device.

Note When using the vSphere Client to register a virtual device to a Defense Center, you must use the IP address (not the hostname) of the managing Defense Center.

However, if the device and the Defense Center are separated by a Network Address Translation (NAT) device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the IP address, for example:

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

where *my_reg_key* is the registration key you entered for the virtual device and *my_nat_id* is the NAT ID of the NAT device.

To register a virtual device to a Defense Center:

Access: CLI Configuration

Step 1 Log into the virtual device as a user with CLI Configuration (Administrator) privileges:

- If you are performing the initial setup from the VMware console, you are already logged in as the `admin` user, which has the required access level.
- Otherwise, log into the device using the VMware console, or, if you have already configured network settings for the device, SSH to the device's management IP address or host name.

Step 2 At the prompt, register the device to a Defense Center using the `configure manager add` command, which has the following syntax:

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE} reg_key
[nat_id]
```

where:

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` specifies the IP address of the Defense Center. If the Defense Center is not directly addressable, use `DONTRESOLVE`.
- *reg_key* is the unique alphanumeric registration key required to register a device to the Defense Center.
- *nat_id* is an optional alphanumeric string used during the registration process between the Defense Center and the device. It is required if the hostname is set to `DONTRESOLVE`.

Step 3 Log out of the appliance.

Step 4 Your next step depends on whether you have already set up the managing Defense Center, and on the Defense Center's model:

- If you have already set up the Defense Center, log into its web interface and use the Device Management (**Devices > Device Management**) page to add the device. For more information, see the Managing Devices chapter in the *FireSIGHT System User Guide*.
- If you have not already set up the Defense Center, see Setting Up a Virtual Defense Center, page 4-6 for a virtual Defense Center, or see the *FireSIGHT System Installation Guide* for a physical Defense Center.

Setting Up a Virtual Defense Center

The steps required to set up a virtual Defense Center depend on whether you deployed with a VI OVF template or an ESXi OVF template:

- If you deployed with a VI OVF template and used the setup wizard, log into the virtual Defense Center using the password you set when you configured the FireSIGHT System-required settings, then use the FireSIGHT System to set local appliance configurations, add licenses and devices, and apply policies to monitor and manage traffic. See the *FireSIGHT System User Guide* for more information.
- If you deployed with an ESXi OVF template or did not configure FireSIGHT System-required settings when deploying with a VI OVF template deployment, setting up a virtual Defense Center is a two-step process. After you initialize the virtual Defense Center, run a script at the VMware

console that helps you configure the appliance to communicate on your management network. Then, complete the setup process using a computer on your management network to browse to the appliance's web interface.

- If you deploy the virtual Defense Center with the ESXi OVF template and deploy all the virtual devices with the VI OVF template, you can register all the devices at the same time to the virtual Defense Center through the one page setup wizard. See Initial Setup Page: Virtual Defense Centers, page 4-8 for more information.

For more information, see:

- Automating Virtual Defense Center Network Settings, page 4-7
- Initial Setup Page: Virtual Defense Centers, page 4-8

Automating Virtual Defense Center Network Settings

After you initialize a new virtual Defense Center, you must configure settings that allow the appliance to communicate on your management network. Complete this step by running a script at the VMware console.

The FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. First, the script prompts you to configure (or disable) IPv4 management settings, then IPv6. For IPv6 deployments, you can retrieve settings from a local router. You must provide the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway.

When following the script's prompts, for multiple-choice questions, your options are listed in parentheses, such as `(y/n)`. Defaults are listed in square brackets, such as `[y]`. Press Enter to confirm a choice.

To configure the Defense Center's network settings using a script:

Access: Admin

Step 1 After the initialization process completes, log into the virtual Defense Center at the VMware console using `admin` as the username and the password for the admin account that you specified in the setup wizard when you deployed with a VI OVF template.

If you did not change the password using the wizard, or you are deploying with an ESXi OVF template, use `Cisco` as the password.

Step 2 At the admin prompt, run the following script:

```
sudo /usr/local/sf/bin/configure-network
```

Step 3 Follow the script's prompts.

First configure (or disable) IPv4 management settings, then IPv6. If you manually specify network settings, you must:

- enter IPv4 addresses, including the netmask, in dotted decimal form. For example, you could specify a netmask of `255.255.0.0`.
- enter IPv6 addresses in colon-separated hexadecimal form. For an IPv6 prefix, specify the number of bits; for example, a prefix length of `112`.

Step 4 Confirm that your settings are correct.

If you entered settings incorrectly, type `n` at the prompt and press Enter. You can then enter the correct information. The VMware console may display messages as your settings are implemented.

Step 5 Log out of the appliance.

Step 6 Continue with Initial Setup Page: Virtual Defense Centers, page 4-8 to complete the setup using the Defense Center's web interface.

Initial Setup Page: Virtual Defense Centers

For virtual Defense Centers, you must complete the setup process by logging into the Defense Center's web interface and specifying initial configuration options on a setup page. You must change the administrator password, specify network settings if you have not already, and accept the EULA.

The setup process also allows you to register and license devices. Before you can register a device, you must complete the setup process on the device itself, as well as add the Defense Center as a remote manager, or the registration will fail.

To complete the initial setup on a Defense Center using its web interface:

Access: Admin

Step 1 From a computer on your management network, direct a supported browser to `https://`*`DC_name`*`/`, where *`DC_name`* is the host name or IP address you assigned to the Defense Center's management interface in the previous procedure.

The login page appears.

Step 2 Log in using `admin` as the username and the password for the admin account that you specified in the setup wizard with a VI OVF template deployment. If you did not change the password using the wizard, use `Cisco` as the password.

The setup page appears. See the following sections for information on completing the setup:

- Change Password, page 4-9
- Network Settings, page 4-9
- Time Settings, page 4-9
- Recurring Rule Update Imports, page 4-9
- Recurring Geolocation Updates, page 4-10
- Automatic Backups, page 4-10
- License Settings, page 4-10
- Device Registration, page 4-11
- End User License Agreement, page 4-12

Step 3 When you are finished, click **Apply**.

The Defense Center is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role.

Step 4 Use the Task Status page (**System > Monitoring > Task Status**) to verify that the initial setup was successful.

The page auto-refreshes every ten seconds. Monitor the page until it lists a status of **Completed** for any initial device registration and policy apply tasks. If, as part of setup, you configured an intrusion rule or geolocation update, you can also monitor those tasks.

The Defense Center is ready to use. See the *FireSIGHT System User Guide* for more information on configuring your deployment.

Step 5 Continue with Next Steps, page 4-12.

Change Password

You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted. Cisco recommends that you use a strong password that is at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

Network Settings

A Defense Center's network settings allow it to communicate on your management network. Because you already used a script to configure the network settings, this section of the page should be pre-populated.

If you want to change the pre-populated settings, remember that the FireSIGHT System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays various fields where you must set the IPv4 or IPv6 management IP address, netmask or prefix length, and default gateway:

- For IPv4, you must set the address and netmask in dotted decimal form (for example: a netmask of `255.255.0.0`).
- For IPv6 networks, you can select the **Assign the IPv6 address using router autoconfiguration** check box to automatically assign IPv6 network settings. Otherwise, you must set the address in colon-separated hexadecimal form and the number of bits in the prefix (for example: a prefix length of `112`).

You can also specify up to three DNS servers, as well as the host name and domain for the device.

Time Settings

You can set the time for a Defense Center either manually or via network time protocol (NTP) from an NTP server.

You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Cisco recommends that you use a physical NTP server to set your time.

Recurring Rule Update Imports

As new vulnerabilities become known, the Cisco Vulnerability Research Team (VRT) releases intrusion rule updates. Rule updates provide new and updated intrusion rules and preprocessor rules, modified states for existing rules, and modified default intrusion policy settings. Rule updates may also delete rules and provide new rule categories and system variables.

If you plan to perform intrusion detection and prevention in your deployment, Cisco recommends that you **Enable Recurring Rule Update Imports**.

You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, select **Install Now**.

Note Rule updates may contain new binaries. Make sure your process for downloading and installing rule updates complies with your security policies. In addition, rule updates may be large, so make sure to import rules during periods of low network use.

Recurring Geolocation Updates

You can use virtual Defense Centers to view geographical information about the routed IP addresses associated with events generated by the system, as well as monitor geolocation statistics in the dashboard and Context Explorer.

The Defense Center's geolocation database (GeoDB) contains information such as an IP address's associated Internet service provider (ISP), connection type, proxy information, and exact location. Enabling regular GeoDB updates ensures that the system uses up-to-date geolocation information. If you plan to perform geolocation-related analysis in your deployment, Cisco recommends that you **Enable Recurring Weekly Updates**.

You can specify the weekly update frequency for the GeoDB. Click the time zone to change it using a pop-up window. To download the database as part of the initial configuration process, select **Install Now**.

Note GeoDB updates may be large and may take up to 45 minutes to install after download. You should update the GeoDB during periods of low network use.

Automatic Backups

The Defense Center provides a mechanism for archiving data so configurations can be restored in case of failure. As part of the initial setup, you can **Enable Automatic Backups**.

Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the Defense Center.

License Settings

You can license a variety of features to create an optimal FireSIGHT System deployment for your organization. A FireSIGHT license on the Defense Center is required to perform host, application, and user discovery. Additional model-specific licenses allow your managed devices to perform a variety of functions. Because of architecture and resource limitations, not all licenses can be applied to all managed devices; see Understanding Virtual Appliance Capabilities, page 1-3 and Licensing Virtual Appliances, page 1-10.

Cisco recommends that you use the initial setup page to add the licenses your organization has purchased. If you do not add licenses now, any devices you register during initial setup are added to the Defense Center as unlicensed; you must then license each of them individually after the initial setup process is over.

Tip If you recreated a virtual Defense Center and used the same MAC address for its management interface as the deleted appliance, you can use your old licenses. If you could not use the same MAC address (for example, it was dynamically assigned), contact Support for new licenses.

If you have not already obtained your licenses, click the link to navigate to https://keyserver.sourcefire.com/ and follow the on-screen instructions. You need your license key (listed on the initial setup page), as well as the activation key previously emailed to the contact associated with your support contract.

Add a license by pasting it into the text box and clicking **Submit License**. After you add a valid license, the page updates so you can track which licenses you have added. Add licenses one at a time.

Device Registration

A virtual Defense Center can manage any device, physical or virtual, currently supported by the FireSIGHT System. You can add most pre-registered devices to the Defense Center during the initial setup process. However, if a device and the Defense Center are separated by a NAT device, you must add it after the setup process completes.

When you register devices, leave the **Apply Default Access Control Policies** check box enabled if you want to apply access control policies to devices upon registration. Note that you cannot choose which policy the Defense Center applies to each device, only whether to apply them. The policy that is applied to each device depends on the detection mode you chose when configuring the device, as listed in the following table.

Table 4-2 Default Access Control Policy Applied Per Detection Mode

Detection Mode	Default Access Control Policy
Inline	Default Intrusion Prevention
Passive	Default Intrusion Prevention
Access Control	Default Access Control
Network Discovery	Default Network Discovery

An exception occurs if you previously managed a device with a Defense Center and you changed the device's initial interface configuration. In this case, the policy applied by this new Defense Center page depends on the changed (current) configuration of the device. If there are interfaces configured, the Defense Center applies the Default Intrusion Prevention policy, otherwise, the Defense Center applies the Default Access Control policy.

For more information on detection modes on virtual devices, see Setting Up a Virtual Device Using the CLI, page 4-3; for physical devices, see the *FireSIGHT System Installation Guide*.

To add a device, type its **Hostname** or **IP Address**, as well as the **Registration Key** you specified when you registered the device. Remember this is a simple key that you specified, and is not the same as a license key.

Then, use the check boxes to add licensed capabilities to the device. Note that you can only select licenses you have already added to the Defense Center. Also, you cannot enable certain licenses until you enable others. For example, you cannot enable Control on a device until you first enable Protection.

Because of architecture and resource limitations, not all licenses can be applied to all managed devices. However, the setup page does **not** prevent you from enabling unsupported licenses on managed devices, or enabling a capability for which you do not have a model-specific license. This is because the Defense Center does not determine the device model until later. The system cannot enable an invalid license, and attempting to enable an invalid license does not decrement your available license count. For more information, see Understanding Virtual Appliance Capabilities, page 1-3 and Licensing Virtual Appliances, page 1-10.

Note If you enabled **Apply Default Access Control Policies**, you must enable a Protection license on the devices where you chose an **Inline** or **Passive** detection mode. You must also enable Protection on any previously managed device that has configured interfaces. Otherwise, the default policy (which requires Protection in those cases) will fail to apply.

After you enable licenses, click **Add** to save the device's registration settings and, optionally, add more devices.

If you selected the wrong options or mis-typed a device name, click **Delete** to remove it. You can then re-add the device.

End User License Agreement

Read the EULA carefully and, if you agree to abide by its provisions, select the check box. Make sure that all the information you provided is correct, and click **Apply**.

The Defense Center is configured according to your selections. After an intermediate page appears, you are logged into the web interface as the `admin` user, which has the Administrator role. Continue with step 3 in Initial Setup Page: Virtual Defense Centers, page 4-8 to complete the initial setup of the Defense Center.

Next Steps

After you complete the initial setup process for a virtual appliance and verify its success, Cisco recommends that you complete various administrative tasks that make your deployment easier to manage. You should also complete any tasks you skipped during the initial setup, such as device registration and licensing. For detailed information on any of the tasks described in the following sections, as well as information on how you can begin to configure your deployment, see the *FireSIGHT System User Guide*.

Individual User Accounts

After you complete the initial setup, the only user on the system is the `admin` user, which has the Administrator role and access. Users with that role have full menu and configuration access to the system, including via the shell or CLI. Cisco recommends that you limit the use of the `admin` account (and the Administrator role) for security and auditing reasons.

Creating a separate account for each person who will use the system allows your organization not only to audit actions and changes made by each user, but also to limit each person's associated user access role or roles. This is especially important on the Defense Center, where you perform most of your configuration and analysis tasks. For example, an analyst needs access to event data to analyze the security of your network, but may not require access to administrative functions for the deployment.

The system includes ten predefined user roles designed for a variety of administrators and analysts. You can also create custom user roles with specialized access privileges.

Health and System Policies

By default, all appliances have an initial system policy applied. The system policy governs settings that are likely to be similar for multiple appliances in a deployment, such as mail relay host preferences and time synchronization settings. Cisco recommends that you use the Defense Center to apply the same system policy to itself and all the devices it manages.

By default, the Defense Center also has a health policy applied. A health policy, as part of the health monitoring feature, provides the criteria for the system continuously monitoring the performance of the appliances in your deployment. Cisco recommends that you use the Defense Center to apply a health policy to all the devices it manages.

Software and Database Updates

You should update the system software on your appliances before you begin any deployment. Cisco recommends that all the appliances in your deployment run the most recent version of the FireSIGHT System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

Caution Before you update any part of the FireSIGHT System, you **must** read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

CHAPTER 5

Troubleshooting Your Virtual Appliance Deployment

This chapter provides information about the most common setup issues, as well as where to submit questions or obtain assistance:

- Time Synchronization, page 5-1
- Performance Issues, page 5-1
- Connectivity Issues, page 5-1
- Inline Interface Configurations, page 5-3
- For Assistance, page 5-3

Time Synchronization

If your health monitor indicates that the clock setup for your virtual appliance is not synchronized, check your system policy time synchronization settings. Cisco recommends that you synchronize your virtual appliances to a physical NTP server. Do not synchronize your managed devices (virtual or physical) to a Virtual Defense Center. To ensure your time synchronization is set up correctly, see Synchronizing Time in the *FireSIGHT System User Guide*. After you determine that the clock setup for your virtual appliance is correct, contact your ESXi host administrator and ensure that the server's time configuration is correct.

Performance Issues

If you are having performance issues, remember that there are several factors that affect your virtual appliance. See Virtual Appliance Performance, page 1-6 for a list of the factors that may affect your performance. To monitor ESXi host performance, you can use your vSphere Client and the information found under the **Performance** tab.

Connectivity Issues

You can view and confirm connectivity for the management and sensing interfaces using VMware vCloud Director Web Portal and vSphere Client.

Using VMware vCloud Director Web Portal

You can use VMware vCloud Director web portal to view and confirm that the management connection and sensing interfaces are properly connected.

To confirm connectivity:

Step 1 Select **My Cloud > VMs**, hover over the virtual appliance you want to view, and right-click.

The Actions window appears.

Step 2 On the Actions window, click **Properties**.

The Virtual Machine Properties window appears.

Step 3 On the **Hardware** tab, view the NICs for the management and sensing interfaces to confirm connectivity.

Using vSphere Client

You can use vSphere Client to confirm that the management connection and sensing interfaces are properly connected.

Management Connection

During initial setup, it is important to ensure that network adapter connects at power on. If you do not, the initial management connection setup cannot properly complete and ends with the message:

```
ADDRCONF (NETDEV_UP): eth0 : link is not ready
```

To ensure that the management connection is connected:

Step 1 Right-click the name of the virtual appliance in the vSphere Client and select **Edit Settings** from the context menu that appears. Select **Network adapter 1** in the **Hardware** list and make sure the **Connect at power on** check box is selected.

When the initial management connection completes properly, check the `/var/log/messages` directory for this message:

```
ADDRCONF (NETDEV_CHANGE): eth0 : link becomes ready
```

Sensing Interfaces

During initial setup, it is important to ensure that sensing interfaces connect at power on.

To ensure that the sensing interfaces connect at power on:

Step 1 Right-click the name of the virtual device in the vSphere Client and select **Edit Settings** from the context menu that appears. Select **Network adapter 2** and **Network adapter 3** in the **Hardware** list. Make sure the **Connect at power on** check box is selected for each adapter in use.

You must connect your virtual device sensing interfaces to a virtual switch or virtual switch group that accepts promiscuous mode traffic. If it is not, your device can detect only broadcast traffic. To ensure your sensing interfaces detect all exploits, see Configuring Virtual Device Interfaces, page 3-9.

Inline Interface Configurations

You can verify that your inline interfaces are symmetrical and that traffic is flowing between them. To open the VMware console to your virtual device, use either VMware vCloud Director web portal or vSphere Client.

To ensure that the inline sensing interfaces are configured properly:

Access: CLI Configuration

Step 1 At the console, log in as a user with CLI Configuration (Administrator) privileges.

The CLI prompt appears.

Step 2 Type `expert` to display the shell prompt.

Step 3 Enter the command: `cat /proc/sf/sfe1000.*`

A text file appears with information similar to this example:

```
SFE1000 driver for eth1 is Fast, has link, is bridging, not MAC filtering, MAC timeout
7500, Max Latency 0.
  39625470 packets received.
         0 packets dropped by user.
  13075508 packets sent.
0 Mode 1 LB Total 0 Bit 000...
.
.
SFE1000 driver for eth2 is Fast, has link, is bridging, not MAC filtering, MAC timeout
7500, Max Latency 0.
  13075508 packets received.
         0 packets dropped by user.
  39625470 packets sent.
0 Mode 1 LB Total 0 Bit 00
```

Note that the number of packets received on `eth1` matches those sent from `eth2` and those sent from `eth1` match those received on `eth2`.

Step 4 Log out of the virtual device.

Step 5 Optionally, and if direct routing to the protected domain is supported, ping the protected virtual appliance where the inline interface of the virtual device is connected.

Pings return to indicate there is connectivity through the inline interface set of the virtual device.

For Assistance

Thank you for using Cisco products.

Sourcefire Support

If you have any questions or require assistance with the FireSIGHT virtual device or virtual Defense Center, please contact Sourcefire Support:

- Visit the Sourcefire Support Site at https://support.sourcefire.com/.
- Email Sourcefire Support at support@sourcefire.com.
- Call Sourcefire Support at 1.410.423.1901 or 1.800.917.4134.

Cisco Support

If you have any questions or require assistance with the Cisco ASA appliances, please contact Cisco Support:

- Visit the Cisco Support Site at http://www.cisco.com/cisco/web/support/index.html.
- Email Cisco Support at tac@cisco.com.
- Call Cisco Support at 1.408.526.7209 or 1.800.553.2447.