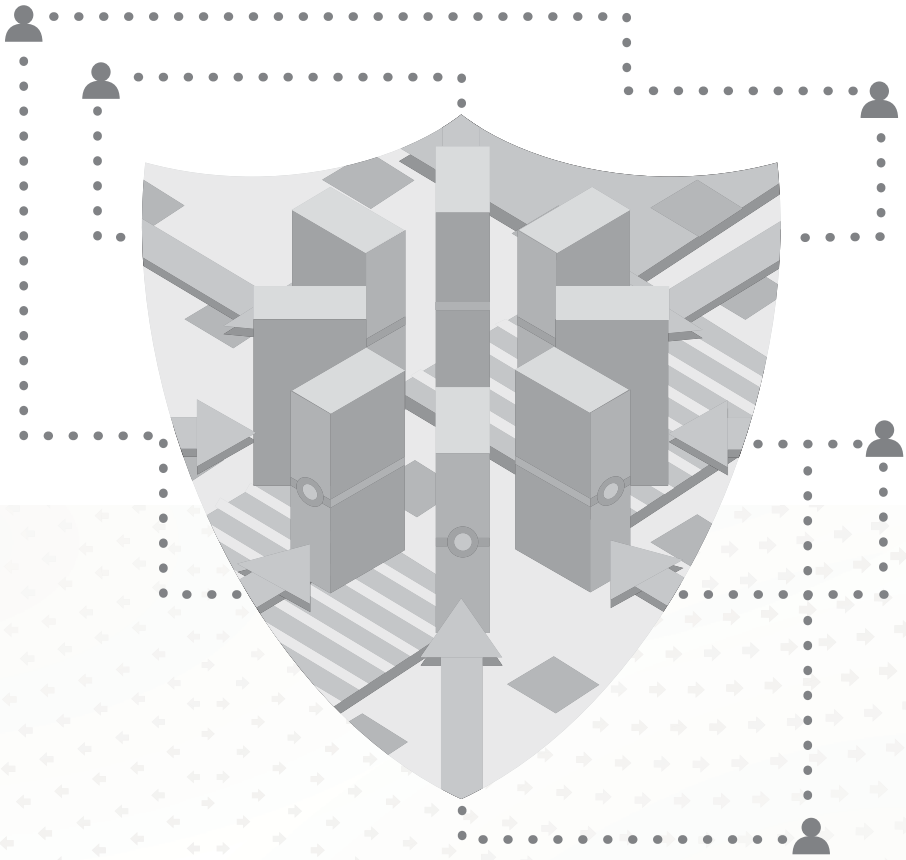
Sourcefire 3D System

Virtual Installation Guide

Version 5.2



SOURCEfire®

Sourcefire is now part of Cisco. CISCO

Legal Notices

Cisco, the Cisco logo, Sourcefire, the Sourcefire logo, Snort, the Snort and Pig logo, and certain other trademarks and logos are trademarks or registered trademarks of Cisco and/or its affiliates in the United States and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Cisco or its subsidiaries (collectively, "Cisco") or any Sourcefire-provided or Cisco-provided products. Sourcefire and Cisco products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

The copyright in the Documentation is owned by Cisco and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Cisco's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

No part of the Documentation may be used in a compilation or otherwise incorporated into another work or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of Cisco. Cisco reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms.

Disclaimers

THE DOCUMENTATION AND ANY INFORMATION AVAILABLE FROM IT MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. CISCO MAY CHANGE THE DOCUMENTATION FROM TIME TO TIME. CISCO MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY CISCO-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION. CISCO-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND CISCO DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL CISCO BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO CISCO-CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF CISCO IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

2014-Mar-25 11:56

Table of Contents

CHAPTER 1
INTRODUCTION TO THE SOURCEFIRE 3D SYSTEM

The Sourcefire 3D® 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.

Sourcefire packages 64-bit virtual Defense Centers® and virtual devices for the VMware ESX/ESXi hosting environment. 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, 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 Sourcefire appliances, see the *Sourcefire 3D System Installation Guide*.

This installation guide provides information about deploying, installing, and setting up virtual Sourcefire appliances (devices and Defense Centers). It also assumes familiarity with the features and nomenclature of VMware products, especially ESX/ESXi and the vSphere Client.

The topics that follow introduce you to Sourcefire 3D System virtual appliances:

Sourcefire 3D System Virtual Appliances

A Sourcefire *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

The Defense Center provides a centralized management point and event database for your Sourcefire 3D System deployment. Virtual Defense Centers aggregate and correlate intrusion, file, malware, discovery, connection, and performance data. 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
- display of event and contextual information using tables, graphs, and charts
- health and performance monitoring
- external notification and alerting
- real-time threat response using correlation and remediation features
- reporting

Virtual Managed Devices

Virtual Sourcefire 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.

Virtual devices can gather detailed information about your organization's hosts, operating systems, applications, users, networks, and vulnerabilities. With additional licensed capabilities, they can block or allow network traffic based on various network-based criteria, as well as other criteria including applications, users, URLs, IP address reputation, files, and results of an intrusion or malware inspection.

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.

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.

The Supported Capabilities by Appliance Model table below matches the major capabilities of the system with the appliances that support those capabilities, assuming you have the correct licenses installed and applied. For a brief summary of the features and licenses supported with virtual appliances, see Sourcefire 3D System Components on page 11 and Licensing Sourcefire Virtual Appliances on page 13.

Keep in mind that virtual Defense Centers can manage Series 2 and Series 3 devices. Similarly, Series 2 and Series 3 Defense Centers can manage virtual devices. The Defense Center columns for device-based capabilities (such as stacking, switching, and routing) indicates whether that Defense Center can manage and configure devices to perform their 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. Also, a blank cell means

the feature is unsupported, while `n/a` marks certain Defense Center-based features that are not relevant to managed devices.

Supported Capabilities by Appliance Model

Feature	Virtual Device	Virtual Defense Center	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center
network discovery: host, application, and user	✓	✓	✓	✓	✓	✓
geolocation data	✓	✓	✓	DC1000, DC3000	✓	✓
intrusion detection and prevention (IPS)	✓	✓	✓	✓	✓	✓
Security Intelligence filtering	✓	✓		DC1000, DC3000	✓	✓
access control: basic network control	✓	✓	✓	✓	✓	✓
access control: applications	✓	✓		✓	✓	✓
access control: users	✓	✓		DC1000, DC3000	✓	✓
access control: literal URLs	✓	✓		✓	✓	✓
access control: URL filtering by category and reputation	✓	✓		DC1000, DC3000	✓	✓
file control: by file type	✓	✓	✓	✓	✓	✓
network-based advanced malware protection (AMP)	✓	✓		DC1000, DC3000	✓	✓
FireAMP integration	n/a	✓	n/a	✓	n/a	✓
fast-path rules		✓	3D9900	✓	8000 Series	✓

Supported Capabilities by Appliance Model (Continued)

Feature	Virtual Device	Virtual Defense Center	Series 2 Device	Series 2 Defense Center	Series 3 Device	Series 3 Defense Center
strict TCP enforcement		✓		✓	✓	✓
configurable bypass interfaces		✓	✓	✓	except where hardware limited	✓
tap mode		✓	3D9900	✓	✓	✓
switching and routing		✓		✓	✓	✓
NAT policies		✓		✓	✓	✓
VPN		✓		✓	✓	✓
high availability	n/a		n/a	DC1000, DC3000	n/a	DC1500, DC3500
device stacking		✓	3D9900	✓	3D8140, 82xx Family	✓
device clustering		✓		✓	✓	✓
clustered stacks		✓		✓	3D8140, 82xx Family	✓
interactive CLI	✓				✓	

Operating Environment Prerequisites

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

- VMware ESX/ESXi 4.1
- VMware ESXi 5.0
- VMware ESXi 5.1

For help creating a hosting environment, see the VMware ESX/ESXi documentation.

Sourcefire virtual appliances use Open Virtual Format (OVF) packaging. VMware Workstation, Player, Server, and Fusion do not recognize OVF packaging and are

not supported. Additionally, Sourcefire virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware.

The computer that serves as the hypervisor 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 hypervisor 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.

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 hypervisor host
- number of total virtual machines running on the hypervisor 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 hypervisor 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 hypervisor host.

Although Sourcefire 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 hypervisor 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.

Sourcefire 3D 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 *Sourcefire 3D System Installation Guide* and the *Sourcefire 3D System User Guide*.

TIP! Many virtual appliance capabilities are license and user role dependent. Where needed, Sourcefire documentation outlines the requirements for each feature and task.

FireSIGHT

FireSIGHT™ is Sourcefire'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.

Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that traverses your network. 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 deeper analysis.

After Security Intelligence filtering occurs, you can define which and how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. You can trust, monitor, or block traffic, or perform further analysis, such as:

- intrusion detection and prevention
- file control
- file tracking and network-based advanced malware protection (AMP)

Intrusion Detection and Prevention

Intrusion detection and prevention is a policy-based feature, integrated into access control, that allows you to monitor your network traffic for security violations and, in inline deployments, to block or alter malicious traffic. 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 Sourcefire 3D System's file control, network file trajectory, and advanced malware protection components can detect, track, and optionally block the transmission of files (including malware files) in network traffic.

File control is a policy-based feature, integrated into access control, that allows managed devices to detect and block your users from uploading (sending) or downloading (receiving) files of specific types over specific application protocols.

Network-based advanced malware protection (AMP) allows the system to inspect network traffic for malware in specific types of files. When a managed device detects one of these file types, the Defense Center obtains the file's disposition from the Sourcefire cloud. The managed device uses this information to track and

then block or allow the file.

FireAMP is Sourcefire's enterprise-class, endpoint-based AMP solution. If your organization has a FireAMP subscription, individual users install FireAMP Connectors on their computers and mobile devices. These lightweight agents communicate with the Sourcefire cloud, which in turn communicates with the Defense Center. In this way, you can use the Defense Center to view malware detection and quarantines on the endpoints in your organization, as well as to track the malware's trajectory.

Application Programming Interfaces

There are several ways to interact with the system using application programming interfaces (APIs):

- The Event Streamer (eStreamer) allows you to stream several kinds of event data from a Sourcefire appliance to a custom-developed client application.
- 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.
- 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.
- Remediations are programs that your Defense Center can automatically launch when certain conditions on your network are met. 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.

Licensing Sourcefire Virtual Appliances

You can license a variety of features to create an optimal Sourcefire 3D System deployment for your organization. You must use the Defense Center to control licenses for itself and the devices it manages.

Sourcefire 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 on an ESX Host on page 34.

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.

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 Protection and Control licenses.

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 on page 7. 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. Also, a blank cell means the license is unsupported, while `n/a` marks Defense Center-based licenses that are not relevant to managed devices.

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				
Series 3 devices: • 7000 Series • 8000 Series	n/a	✓	✓	✓	✓	✓
virtual devices	n/a	✓	no support for hardware features	✓	✓	
DC500 Series 2 Defense Center	✓	no Security Intelligence	no user control			✓
DC1000/3000 Series 2 Defense Centers	✓	✓	✓	✓	✓	✓
DC750/1500/3500 Series 3 Defense Centers	✓	✓	✓	✓	✓	✓
virtual Defense Centers	✓	✓	✓	✓	✓	✓

For detailed information on licensing, see the Licensing the Sourcefire 3D System chapter in the *Sourcefire 3D System User Guide*.

Security, Internet Access, and Communication Ports

To safeguard a Defense Center, including a virtual Defense Center, you must install 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 from outside the firewall.

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

Note, however, that Sourcefire appliances are configured to directly connect to the Internet. Specific features of the Sourcefire 3D System require this direct connection, and others support use of a proxy server. Additionally, the system requires that certain ports remain open for basic intra-appliance communication, as well as to allow you to access appliances' web interfaces. By default, several other ports are open to allow the system to take advantage of additional features and functionality.

For more information, see:

- Internet Access Requirements on page 16
- Open Communication Ports Requirements on page 17

Internet Access Requirements

By default, Sourcefire appliances are configured to directly connect to the Internet. Specific features of the Sourcefire 3D System require this direct connection, and others support use of a proxy server; see the Configuring Network Settings chapter in the *Sourcefire 3D System User Guide*.

TIP! You can manually upload system software, intrusion rule, GeoDB, and VDB updates to appliances.

The following table describes the Internet access requirements of the Sourcefire 3D System.

Sourcefire 3D System Internet Access Requirements

FOR...	INTERNET ACCESS IS REQUIRED TO...	PROXY?
RSS Feed dashboard widget	download RSS feed data from an external source, including Sourcefire.	✓
Security Intelligence feeds	download Security Intelligence feed data from an external source, including the Sourcefire Intelligence Feed.	✓
URL filtering data	download cloud-based URL category and reputation data for access control, and perform lookups for uncategorized URLs.	✓
malware cloud lookups (Malware licensed)	perform cloud lookups to determine if files detected in network traffic contain malware.	
FireAMP integration (FireAMP subscription)	receive endpoint-based malware events from the Sourcefire cloud.	
system, intrusion rule, GeoDB, and VDB updates	download or schedule the download of an intrusion rule, GeoDB, VDB, or system update directly to the appliance.	✓
obtaining whois information using the IP address context menu	obtain whois information.	✓

Open Communication Ports Requirements

The Sourcefire 3D System requires that ports 443 (inbound) and 8305 (inbound and outbound) remain open for basic intra-appliance communication, as well as to allow you to access the virtual Defense Center's web interface.

By default, several other ports are open to allow the system to take advantage of additional features and functionality. The following table lists these ports. Note that DHCP is disabled by default on ports 67 and 68.

Sourcefire 3D System Open Communication Ports Requirements

Ports	Description	Protocol	Direction	Open the port to...
22	SSH/SSL	TCP	Bidirectional	allow a secure remote connection to the appliance.
25	SMTP	TCP	Outbound	send email notices and alerts from the appliance.
53	DNS	TCP	Outbound	use DNS.
67, 68	DHCP	UDP	Outbound	use DHCP. **Disabled by default.**
80	HTTP	TCP	Outbound or Bidirectional	allow the RSS Feed dashboard widget to connect to a remote web server; use for auto-update. Adding inbound access allows the Defense Center to update custom and third-party Security Intelligence feeds via HTTP, and to download URL filtering information.
161	SNMP	UDP	Bidirectional	provide access if you enabled SNMP polling.
162	SNMP	UDP	Outbound	provide access if you enabled SNMP traps (outbound).
389, 636	LDAP	TCP	Outbound	track user activity and for authentication.
443	HTTPS/AMPQ	TCP	Inbound or Bidirectional	access the appliance. **Required.** Adding outbound access allows the Defense Center to download or receive software updates, VDB and GeoDB updates, URL filtering information, secure Security Intelligence feeds, and endpoint-based (FireAMP) malware events.
514	syslog	UDP	Outbound	send alerts to a remote syslog server.
1500, 2000	database access	TCP	Inbound	access the Defense Center if external database access is enabled.

Sourcefire 3D System Open Communication Ports Requirements (Continued)

Ports	Description	Protocol	Direction	Open the port to...
1812, 1813	RADIUS	UDP	Outbound or Bidirectional	use RADIUS. Adding inbound access ensures that RADIUS authentication and accounting function correctly. Ports 1812 and 1813 are the default, but you can configure RADIUS to use other ports instead. For more information, see the *Sourcefire 3D System User Guide*.
3306	User Agent	TCP	Inbound	allow communication between the Defense Center and Sourcefire User Agents.
8302	eStreamer	TCP	Bidirectional	use for an eStreamer client.
8305	device management	TCP	Bidirectional	communicate between the Defense Center and managed devices. **Required**.
8307	host input client	TCP	Bidirectional	communicate with the Defense Center during client/server authentication.
32137	malware cloud lookups	TCP	Outbound	allow the Defense Center to perform cloud lookups to determine if a file detected in network traffic contains malware.

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 an existing VMware ESX hypervisor 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.

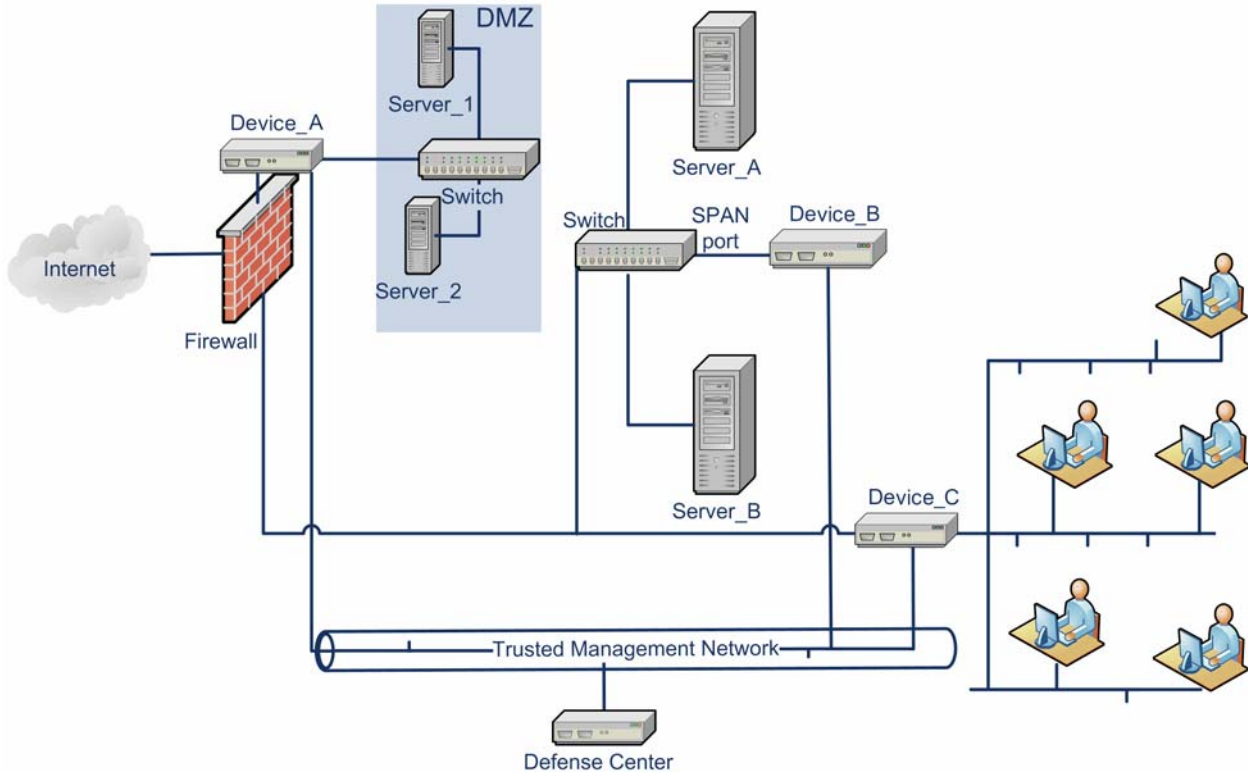
WARNING! Sourcefire **strongly** recommends that you keep your production network traffic and your trusted management network traffic on different network segments. You must take precautions to ensure the security of the appliances and the management traffic data stream.

This chapter provides deployment examples for:

Typical Sourcefire 3D System Deployment

In a physical appliance environment, a typical Sourcefire 3D 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 ESX Virtual Appliance Deployments

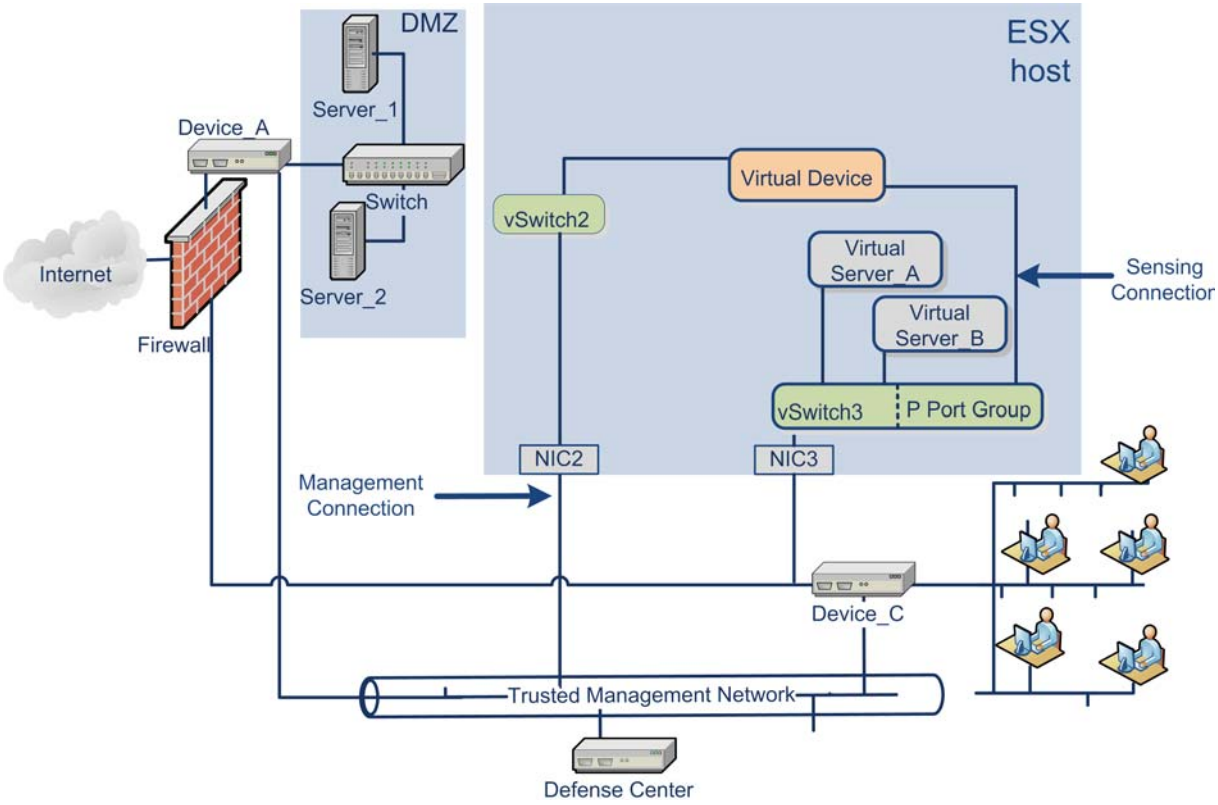
See the following set of ESX virtual appliance deployment scenarios for examples of typical deployments:

Adding Virtualization and a Virtual Device

You can replace the physical internal servers in our Typical Sourcefire 3D System Deployment on page 20 by using virtual infrastructure. In the following example, you can use an ESX 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.



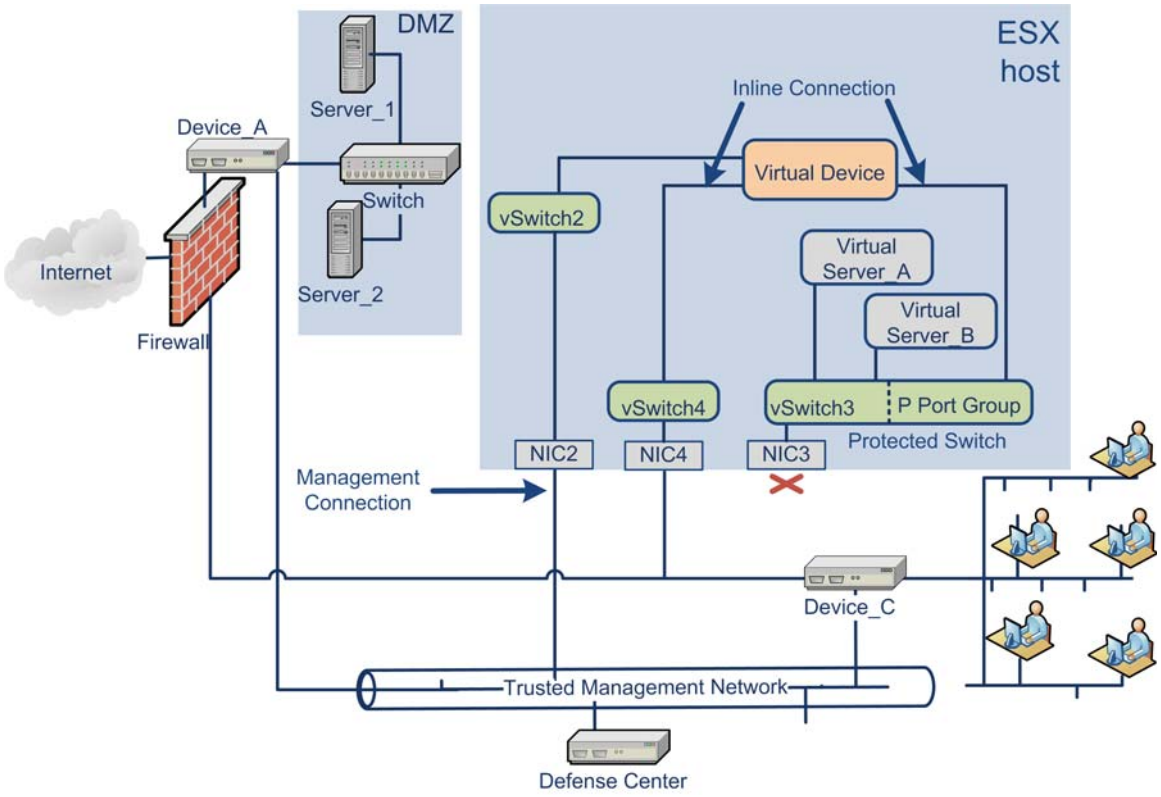
IMPORTANT! To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See Configuring Virtual Device Sensing Interfaces on page 32.

Although our example shows only one sensing interface, three sensing interfaces are available 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 Sourcefire 3D System Deployment on page 20 and on the example shown in Adding Virtualization and a Virtual Device on page 22.

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 *Sourcefire 3D System User Guide*.



IMPORTANT! To sense all traffic, allow promiscuous mode traffic on the virtual switches or port groups where the device sensing interfaces connect. See Configuring Virtual Device Sensing Interfaces on page 32.

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

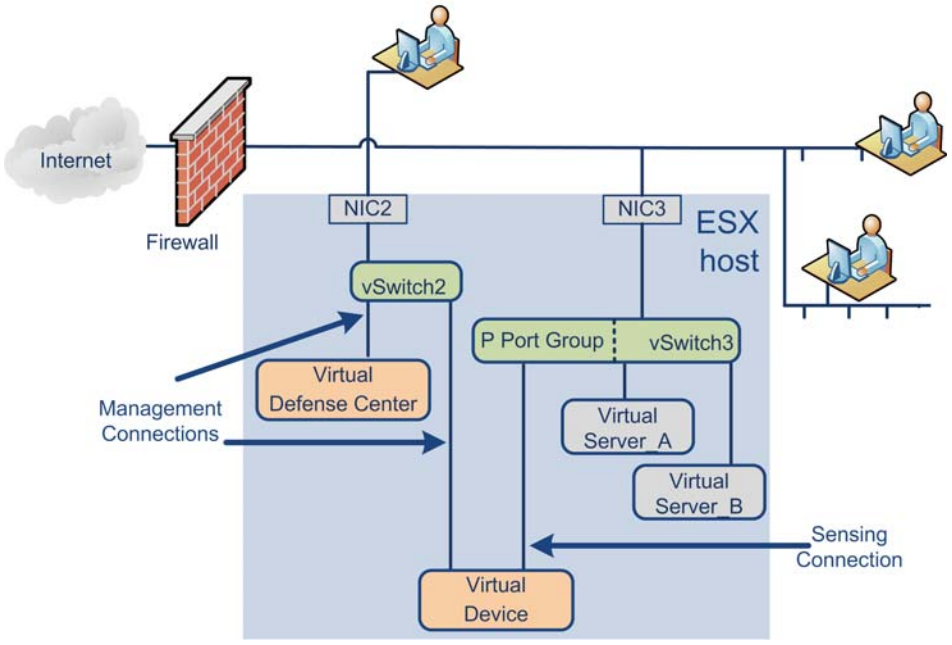
Adding a Virtual Defense Center

You can deploy a virtual Defense Center on the ESX host and connect it to the virtual network as well as the physical network, as shown below. This scenario builds on the Typical Sourcefire 3D System Deployment on page 20 and on the example shown in Using the Virtual Device for Inline Detection on page 23.

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.

Using a Pilot Deployment

Because Sourcefire virtual appliances are preconfigured with the required application software, they are ready to run when deployed on an ESX host. This diminishes complex hardware and software compatibility issues so you can accelerate your deployment and concentrate on the benefits of a Sourcefire 3D System. As a test or pilot, you can deploy virtual servers, a virtual Defense Center, and a virtual device on an ESX host and manage it, as shown below.

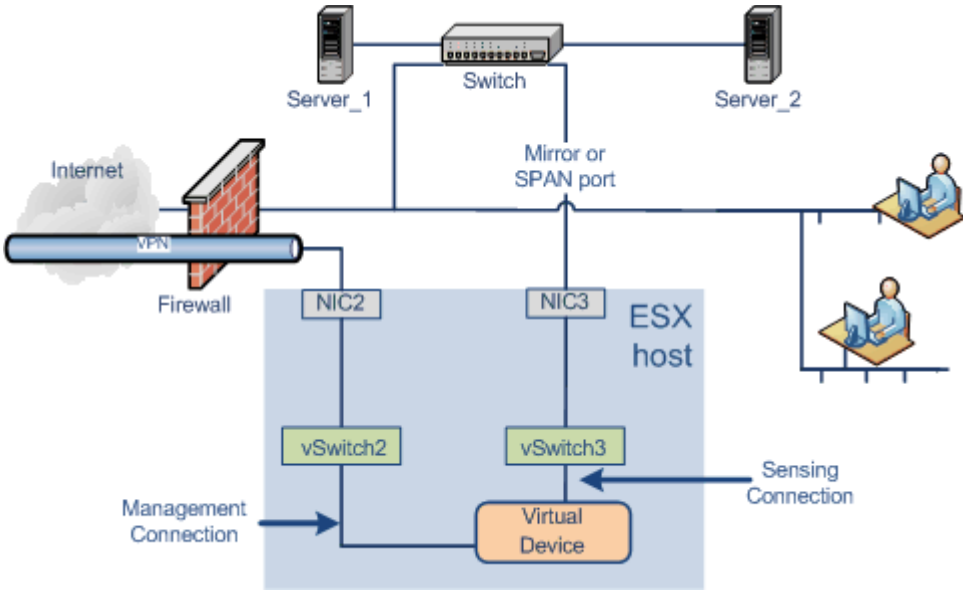


Your sensing connection on your virtual device must be allowed to monitor network traffic. The virtual switch, or the port group on that switch to which the virtual interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In the example, the P Port Group is set to accept promiscuous mode traffic. See Configuring Virtual Device Sensing Interfaces on page 32.

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 ESX host Network Interface Card (NIC2 in our example) allows you to access the virtual Defense Center. See Configuring Virtual Defense Center Network Settings Using a Script on page 40 and Setting Up a Virtual Device on page 36 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 ESX host and monitor local traffic, as shown below.



Your sensing connection on your virtual device must be allowed to monitor network traffic. To do this, the virtual switch, or port group on the switch to which the sensing interface connects, must accept promiscuous mode traffic. This permits the virtual device to read packets intended for other machines or network devices. In our example, all of vSwitch3 is set to accept promiscuous mode traffic. VSwitch3 is also connected through NIC3 to the SPAN port so that it can monitor traffic as it passes through the remote office's switch. See Configuring Virtual Device Sensing Interfaces on page 32.

Your virtual device must be managed by a Defense Center. The connection through the ESX host 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 on page 36 for information on setting up the virtual device management connections.

Chapter 3

Installing Virtual Appliances on an ESX Host

Sourcefire provides packaged virtual appliances for the VMware hosting hypervisor environment on its Support Site as compressed archive (`.tar.gz`) files. Sourcefire virtual appliances are packaged as virtual machines with Version 7 of the virtual hardware.

IMPORTANT! VMware snapshots of Sourcefire virtual appliances are **not** supported.

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

After you install and configure a virtual appliance according to the following procedure, 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 on page 33.

To install and deploy a Sourcefire virtual appliance:

1. Make sure your planned deployment meets the prerequisites described in Operating Environment Prerequisites on page 9.
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 on page 28.
3. Use the VMware vSphere Client to install the virtual appliance, but do not power it on; see Installing a Virtual Appliance on page 29.

4. Confirm and adjust network, hardware, and memory settings; see Updating Important Settings Post-Installation on page 30.
5. Make sure the sensing interfaces on virtual devices are correctly connected to a hypervisor virtual switch; see Configuring Virtual Device Sensing Interfaces on page 32.

Obtaining the Installation Files

Sourcefire 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
- the Manifest File (`.mf`)
- the Virtual Machine Disk Format (`.vmdk`)

Before you install a virtual appliance, obtain the correct archive file from the Sourcefire Support Site. Sourcefire 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, 5.1 or 5.2).

To obtain virtual appliance archive files:

1. Using the user name and password for your support account, log into the Sourcefire Support Site (https://support.sourcefire.com/).
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 5.2 archive file, click **Downloads > 3D System > 5.2**.
3. Find the archive file that 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 **5.2 Virtual Appliances** to view the archive files for Version 5.2 of the Sourcefire 3D System.
4. Click the archive you want to download.

   The file begins downloading.

TIP! While you are logged into the Support Site, Sourcefire 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 rules and Vulnerability Database (VDB) updates.

5. Copy the archive file where the VMware vSphere Client can access it, such as a local hard drive, network share, CD/DVD drive, or a HTTP (web) server.

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

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

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

7. Continue with Installing a Virtual Appliance.

Installing a Virtual Appliance

After you make sure your planned deployment meets the prerequisites described in Operating Environment Prerequisites on page 9 and you download the necessary archive files, use the VMware vSphere Client to install virtual appliances. The following table lists the information the client requires.

VMware vSphere OVF Template

SETTING	ACTION
Import/Deploy OVF Template	Browse to the OVF template you downloaded in the previous procedure.
OVF Template Details	Confirm the appliance you are installing: virtual Defense Center or virtual device.
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.

To install a virtual appliance:

1. Using the VMware vSphere Client, deploy or import the OVF template file you downloaded earlier:
   - For ESX servers, click **File > Deploy OVF Template**.

     The Deploy OVF Template page appears.
   - For ESXi servers, click **File > Virtual Appliances > Import**.

     The Import OVF Template page appears. Click **Import from file**.
2. Follow the client's prompts, providing the information listed in the VMware vSphere OVF Template table on page 29.

   As you complete each prompt, click **Next** to continue.
3. On the Ready to Complete page, confirm your settings and click **Finish**.

   If your deployment settings are not correct, click **Back** and make corrections before you click **Finish**.

   IMPORTANT! Do **not** enable the **Power on after deployment** option. You must complete some additional steps before you power on the appliance.

   A status window appears indicating the installation progress. A status bar appears in the Recent Tasks window at the bottom of the vSphere Client window. When the installation is complete, the appliance is listed in the vSphere Client window.
4. Click **Close** to close the status window.
5. 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.

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:

1. Right-click the name of your new virtual appliance, then select **Edit Settings** from the context menu.

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

2. Make sure the **Memory**, **CPUs**, and **Hard disk 1** settings are set no lower than the defaults, as described in the Default Virtual Appliance Settings table on page 31.

   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**.

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.

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 Network Connection, set the **Network label** to the name of the management network for your virtual appliance.
5. Click **OK**.

   Your changes are saved.
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 on an ESX Host on page 34.
   - A virtual device needs some additional configurations; continue with Configuring Virtual Device Sensing Interfaces.

Configuring Virtual Device Sensing Interfaces

The sensing interfaces on a virtual device must have a network connection to a port on a hypervisor 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 ESX documentation.

To permit promiscuous mode:

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

   The virtual switch diagram appears.
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.
4. On the **Switch Properties** pop-up window, click **Edit**.

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

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 ESX environment, set the VLAN ID of the promiscuous port to 4095.

6. Save your changes.

   The device is ready to initialize.

7. Continue with the next chapter, Setting Up Virtual Appliances on an ESX Host on page 34.

Uninstalling a Virtual Appliance

You may need to uninstall or remove your virtual appliances. Uninstall a virtual appliance from VMware server by deleting it from the disk.

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 Sensing Interfaces on page 32.

To uninstall a virtual appliance:

ACCESS: Admin

1. At the console, log in as a user with Administrator (or, for virtual devices, CLI Configuration) privileges.

   The prompt for the appliance appears.

2. Shut down the virtual appliance:

   - On a virtual Defense Center, type `sudo su -`, then type your password again. At the root prompt, shut down the appliance by typing `shutdown -h now`.
   - On a virtual device, type `system shutdown`.

   The virtual appliance shuts down.

3. After the virtual appliance powers off, click on name of that appliance in the VMware client context menu. With the correct appliance selected, delete it from the disk using the **Inventory** menu. Click **Yes** in the Confirm Delete dialog box.

   The virtual appliance is uninstalled.

CHAPTER 4

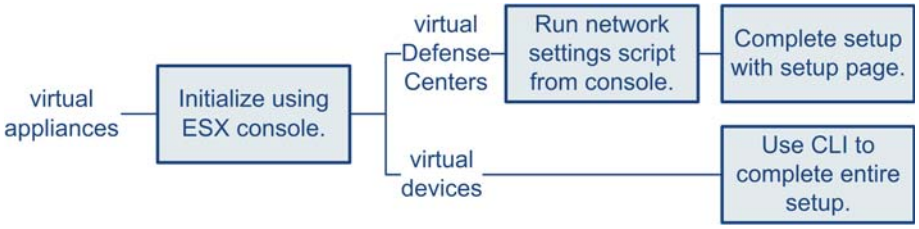
SETTING UP VIRTUAL APPLIANCES ON AN ESX HOST

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.

The following diagram shows the general process of setting up virtual Defense Centers and managed devices.



To begin, power on the appliance to initialize it. After initialization completes, log in using the ESX console and complete the setup in one of the following ways, depending on the appliance type:

Virtual Devices

Because virtual devices do not have web interfaces, use the interactive command line interface (CLI) to perform the entire initial setup and to register virtual devices to a Defense Center.

Virtual Defense Centers

First configure network settings using a script, then 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 on page 35
- Setting Up a Virtual Device on page 36
- Setting Up a Virtual Defense Center on page 40
- Next Steps on page 49

Initializing a Virtual Appliance

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

WARNING! 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.

To initialize a virtual appliance:

1. In the VMware vSphere Client, power on the virtual appliance.

   Right-click the name of your imported virtual appliance from the inventory list, then select **Power > Power On** from the context menu.

2. Monitor the initialization on the Console tab.

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

3. Your next step depends on the appliance type:
   - To set up a virtual device using its CLI, continue with Setting Up a Virtual Device on page 36.
   - To begin setting up a virtual Defense Center by configuring its network settings using a script, continue with Setting Up a Virtual Defense Center on page 40.

Setting Up a Virtual Device

Because virtual devices do not have a web interface, you must use a device's CLI to perform its initial setup after you install and initialize it. When you first log in to 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 *Sourcefire 3D 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 *Sourcefire 3D System User Guide*.

Understanding Device Network Settings

The Sourcefire 3D 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, Security Intelligence monitoring, as well as network discovery.

Inline

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

IMPORTANT! 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.

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 *Sourcefire 3D System User Guide*.

To set up a virtual device using its CLI:

Access: Admin

1. Log in to the appliance at the console. Use `admin` as the username and `Sourcefire` as the password.

   The device immediately prompts you to read the EULA.

2. Read and accept the EULA.

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

   Sourcefire 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.

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 console may display messages as your settings are implemented.

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

   The 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.

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.

   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 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 hostname or the IP address along with the registration key, for example:

```
configure manager add DC.example.com my_reg_key
```

However, if the device and the Defense Center are separated by a NAT device, enter a unique NAT ID along with the registration key, and specify `DONTRESOLVE` instead of the hostname, for example:

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

To register a virtual device to a Defense Center:

Access: CLI Configuration

1. Log in to the virtual device as a user with CLI Configuration (Administrator) privileges:
   - If you are performing the initial setup from the console, you are already logged in as the `admin` user, which has the required access level.
   - Otherwise, log into the device using the ESX console, or, if you have already configured network settings for the device, SSH to the device's management IP address or host name.
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 either the fully qualified host name or 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.`
3. Log out of the appliance.
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 *Sourcefire 3D System User Guide*.
   - If you have not already set up the Defense Center, see Setting Up a Virtual Defense Center on page 40 for a virtual Defense Center, or see the *Sourcefire 3D System Installation Guide* for a physical Defense Center.

Setting Up a Virtual Defense Center

After you install and initialize it, setting up a virtual Defense Center is a two-step process. First, run a script at the ESX 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.

For more information, see:

- Configuring Virtual Defense Center Network Settings Using a Script on page 40
- Initial Setup Page: Virtual Defense Centers on page 41

Configuring Virtual Defense Center Network Settings Using a Script

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 console.

The Sourcefire 3D 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

1. At the console, after the initialization process completes, log in to the Defense Center.

   Use `admin` as the username and `Sourcefire` as the password.

2. At the admin prompt, switch to the root user by typing `sudo su -`, then typing the password again if prompted.

3. At the root prompt, run the following script:

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

4. 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.

5. 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 console may display messages as your settings are implemented.

6. Log out of the appliance.

7. Continue with Initial Setup Page: Virtual Defense Centers on page 41 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 haven't 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

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.

2. Log in using `admin` as the username and `Sourcefire` as the password.

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

   - Change Password on page 42
   - Network Settings on page 43
   - Time Settings on page 44
   - Recurring Rule Update Imports on page 44
   - Recurring Geolocation Updates on page 45
   - Automatic Backups on page 45
   - License Settings on page 46
   - Device Registration on page 47
   - End User License Agreement on page 49

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.

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

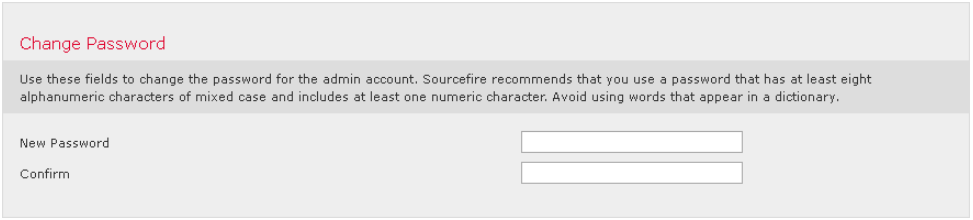
   The page auto-refreshes every ten seconds. Monitor the page until it lists a status of **Completed** for any initial device registration and policy apply tasks. If, as part of setup, you configured an intrusion rule or geolocation update, you can also monitor those tasks.

   The Defense Center is ready to use. See the *Sourcefire 3D System User Guide* for more information on configuring your deployment.

5. Continue with Next Steps on page 49.

Change Password

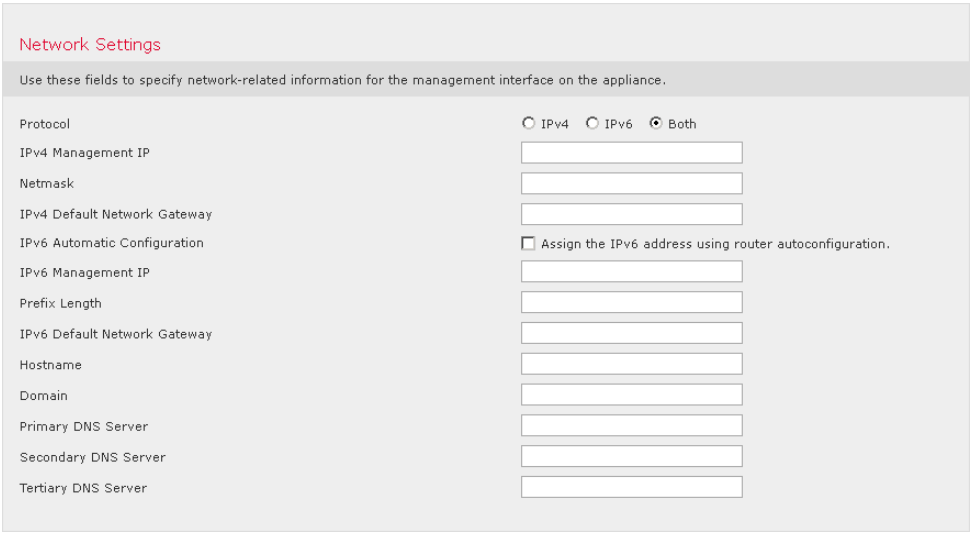
You must change the password for the `admin` account. This account has Administrator privileges and cannot be deleted.



Sourcefire 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.



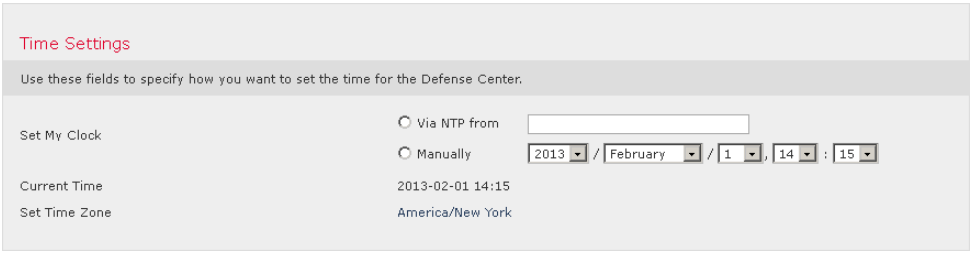
If you want to change the pre-populated settings, remember that the Sourcefire 3D System provides a dual stack implementation for both IPv4 and IPv6 management environments. You must specify the management network protocol (**IPv4**, **IPv6**, or **Both**). Depending on your choice, the setup page displays 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.

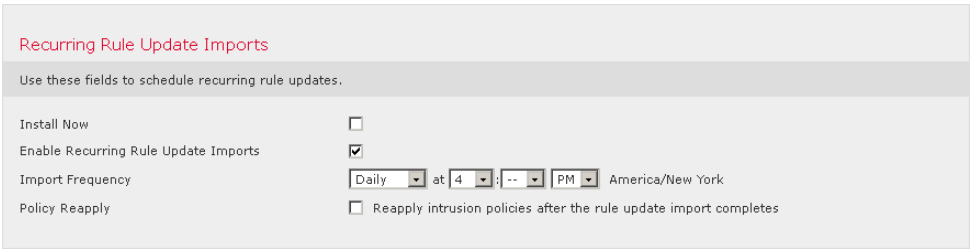


You can also specify the time zone used on the local web interface for the `admin` account. Click the current time zone to change it using a pop-up window.

Recurring Rule Update Imports

As new vulnerabilities become known, the Sourcefire 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, Sourcefire recommends that you **Enable Recurring Rule Update Imports**.



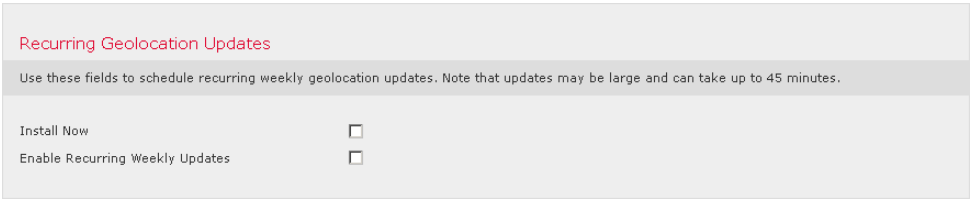
You can specify the **Import Frequency**, as well as configure the system to perform an intrusion **Policy Reapply** after each rule update. To perform a rule update as part of the initial configuration process, select **Install Now**.

IMPORTANT! 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, Sourcefire 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**.

IMPORTANT! 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**.

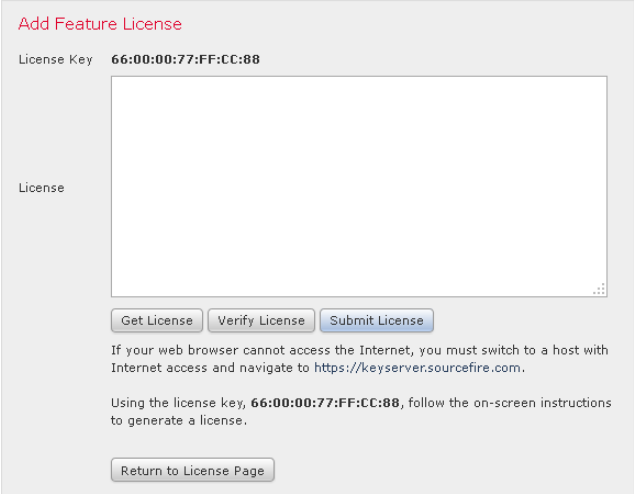
Enabling this setting creates a scheduled task that creates a weekly backup of the configurations on the Defense Center.

License Settings

You can license a variety of features to create an optimal Sourcefire 3D 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 on page 7 and Licensing Sourcefire Virtual Appliances on page 13.

Sourcefire 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.

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**.

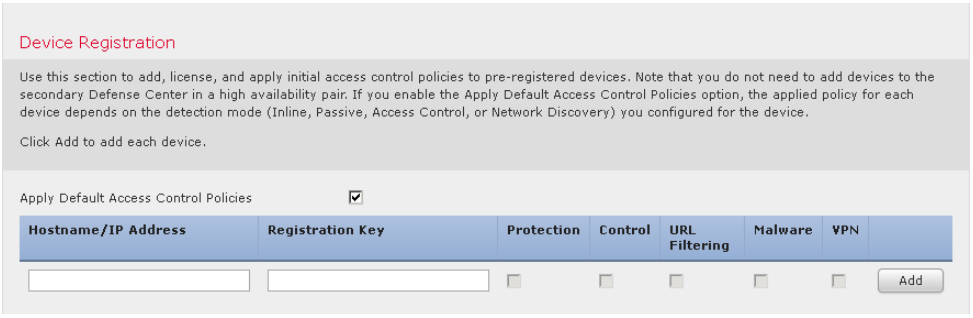
After you add a valid license, the page updates so you can track which licenses you have added. Add licenses one at a time.

Maximum 3D8250 Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	0	5
Maximum Virtual Device 64bit Licenses				
Protection	Control	URL Filtering	Malware	VPN
5	5	0	5	0
Maximum Virtual DC 64bit Licenses				
FireSIGHT Host	FireSIGHT User			
50000	50000			

Type	Description	Expires
3D8250	5 Protection License(s)	Never
3D8250	5 Control License(s)	Never
3D8250	5 VPN License(s)	Never
Virtual Device 64bit	5 Malware License(s)	2013-09-16 18:58:01
Virtual Device 64bit	5 Control License(s)	Never
Virtual Device 64bit	5 Protection License(s)	Never
Virtual DC 64bit	50000 FireSIGHT Host, 50000 FireSIGHT User License(s)	Never

Device Registration

A virtual Defense Center can manage any device, physical or virtual, currently supported by the Sourcefire 3D 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 registering 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.

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 on page 36; for physical devices, see the *Sourcefire 3D 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.

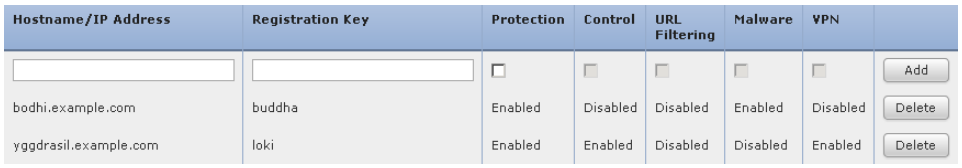
Then, use the check boxes to add licensed capabilities to the device. Note that you can only select licenses you have already added to the Defense Center. Also, you cannot enable certain licenses until you enable others. For example, you cannot enable Control on a device until you first enable Protection.

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 on page 7 and Licensing Sourcefire Virtual Appliances on page 13.

IMPORTANT! 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 on page 41 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, Sourcefire 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 *Sourcefire 3D 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.

Sourcefire 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. Sourcefire 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. Sourcefire 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. Sourcefire recommends that all the appliances in your deployment run the most recent version of the Sourcefire 3D System. If you are using them in your deployment, you should also install the latest intrusion rule updates, VDB, and GeoDB.

WARNING! Before you update any part of the Sourcefire 3D 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

If your health monitor indicates that the clock setup for your virtual appliance is not synchronized, check your system policy time synchronization settings. Sourcefire 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 *Sourcefire 3D System User Guide*. After you determine that the clock setup for your virtual appliance is correct, contact your ESX 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 on page 11 for a list of the factors that may affect your performance. To monitor ESX host performance, you can use your vSphere Client and the information found under the **Performance** tab.

Management Connection on ESX Hosts

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:

- 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 on ESX Hosts

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:

- 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 Sensing Interfaces on page 32.

Inline Interface Configurations on ESX Hosts

You can verify that your inline interfaces are symmetrical and that traffic is flowing between them. To open the console to your virtual device for ESX, use the vSphere Client.

To ensure that the inline sensing interfaces are configured properly:

Access: CLI Configuration

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

   The CLI prompt appears.

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

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`.

4. Log out of the virtual device.

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

If you have any questions or require assistance with the Sourcefire 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 410.423.1901 or 1.800.917.4134.

Thank you for using Sourcefire products.