McAfee® Firewall Enterprise, Multi-Firewall Edition (2150 VX)

Product Guide

McAfee Firewall Enterprise (*Sidewinder®*), Virtual Appliance
version 7.0.1.00

McAfee Firewall Enterprise Control Center (*CommandCenter™*), Virtual Appliance
version 4.0.0.03

McAfee®
An Intel Company

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE AGREEMENT

Contents

About this Guide

The McAfee Firewall Enterprise, Multi-Firewall Edition Product Guide describes the installation and configuration of the Firewall Enterprise, Multi-Firewall Edition 2150 VX appliance.

This guide is intended for network and security administrators. It assumes you possess familiarity with:

- UNIX and Microsoft Windows operating systems
- System administration
- Internet and associated terms and applications
- Networks and network terminology, including TCP/IP protocols

You can find additional information at the following locations:

- **Documentation** – Select **Start > Programs > McAfee > McAfee Firewall Enterprise (Sidewinder) > Online Manuals**.
- **Help** – The Firewall Enterprise GUI (called the Admin Console) provides comprehensive help. To access help, click the help icon in the toolbar.

  Man ("manual") pages provide additional help on firewall-specific commands, file formats, and system routines. To view the available information for a specific topic, enter **`man -k`** *`topic`* or **`apropos`** *`topic`* at the shell prompt.
- **Support** – Visit mysupport.mcafee.com to find product documentation, announcements, and support.

Typographical conventions

This guide uses the following typographic conventions:

Table 1 Conventions

Convention	Description
`Courier bold`	Identifies commands and key words you type at a system prompt Note: A backslash (\) signals a command that does not fit on the same line. Enter the command as shown, ignoring the backslash.

`Courier italic`
`<Courier italic>`
`nnn.nnn.nnn.nnn`
	Indicates a placeholder for text you type
	When enclosed in angle brackets (< >), identifies optional text
	Indicates a placeholder for an IP address you type

`Courier plain`	Used to show text that appears on a computer screen
Plain text italics	Identifies the names of files and directories Used for emphasis (for example, when introducing a new term)
Plain text bold	Identifies buttons, field names, and tabs that require user interaction
[ ]	Signals conditional or optional text and instructions (for example, instructions that pertain only to a specific configuration)
Caution	Be careful—in this situation, you might do something that could result in the loss of data or an unpredictable outcome.
Note	Helpful suggestion or a reference to material not covered elsewhere in the manual
Security Alert	Information that is critical for maintaining product integrity or security
Tip	Time-saving actions; may help you solve a problem

Note: The IP addresses, screen captures, and graphics used within this document are for illustration purposes only. They are not intended to represent a complete or appropriate configuration for your specific needs. Features may be enabled in screen captures to make them clear; however, not all features are appropriate or desirable for your setup.

Acronyms

Refer to Table 2 for a list of acronyms used throughout this document.

Table 2 Acronyms

Acronym	Description
CPU	Central Processing Unit
FQDN	Fully Qualified Domain Name
GUI	Graphical User Interface
HA	High Availability
HR	Human Resources
NIC	Network Interface Card
NTP	Network Time Protocol
NTPD	Network Time Protocol Daemon
OS	Operating System
RFC	Request For Comments
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

1 Introduction to McAfee Firewall Enterprise, Multi-Firewall Edition

Contents

About McAfee Firewall Enterprise, Multi-Firewall Edition

McAfee Firewall Enterprise, Multi-Firewall Edition appliances run VMware ESXi 3.5 Update 3, a hypervisor operating system, to increase flexibility through virtualization. The appliances host 8, 16, or 32 McAfee Firewall Enterprise, Virtual Appliances that have the same capabilities as physical firewalls. Each appliance also hosts a single McAfee Firewall Enterprise Control Center, Virtual Appliance that allows you to centrally manage virtual or physical firewalls.

The following McAfee Firewall Enterprise, Multi-Firewall Edition (2150 VX) appliance models are available:

- **VX-8** – Hosts eight McAfee Firewall Enterprise, Virtual Appliances and a single McAfee Firewall Enterprise Control Center, Virtual Appliance.
- **VX-16** – Hosts 16 McAfee Firewall Enterprise, Virtual Appliances and a single McAfee Firewall Enterprise Control Center, Virtual Appliance.
- **VX-32** – Hosts 32 McAfee Firewall Enterprise, Virtual Appliances and a single McAfee Firewall Enterprise Control Center, Virtual Appliance.

Planning your deployment

This section includes the following deployment scenarios:

- *Consolidated segmentation* on page 7
- *McAfee Firewall Enterprise Control Center management* on page 8
- *Consolidated High Availability* on page 10

Consolidated segmentation

Firewall segmentation can be achieved using a single 2150 VX appliance, providing one Firewall Enterprise, Virtual Appliance per department or business unit.

Consolidated segmentation provides the following benefits:

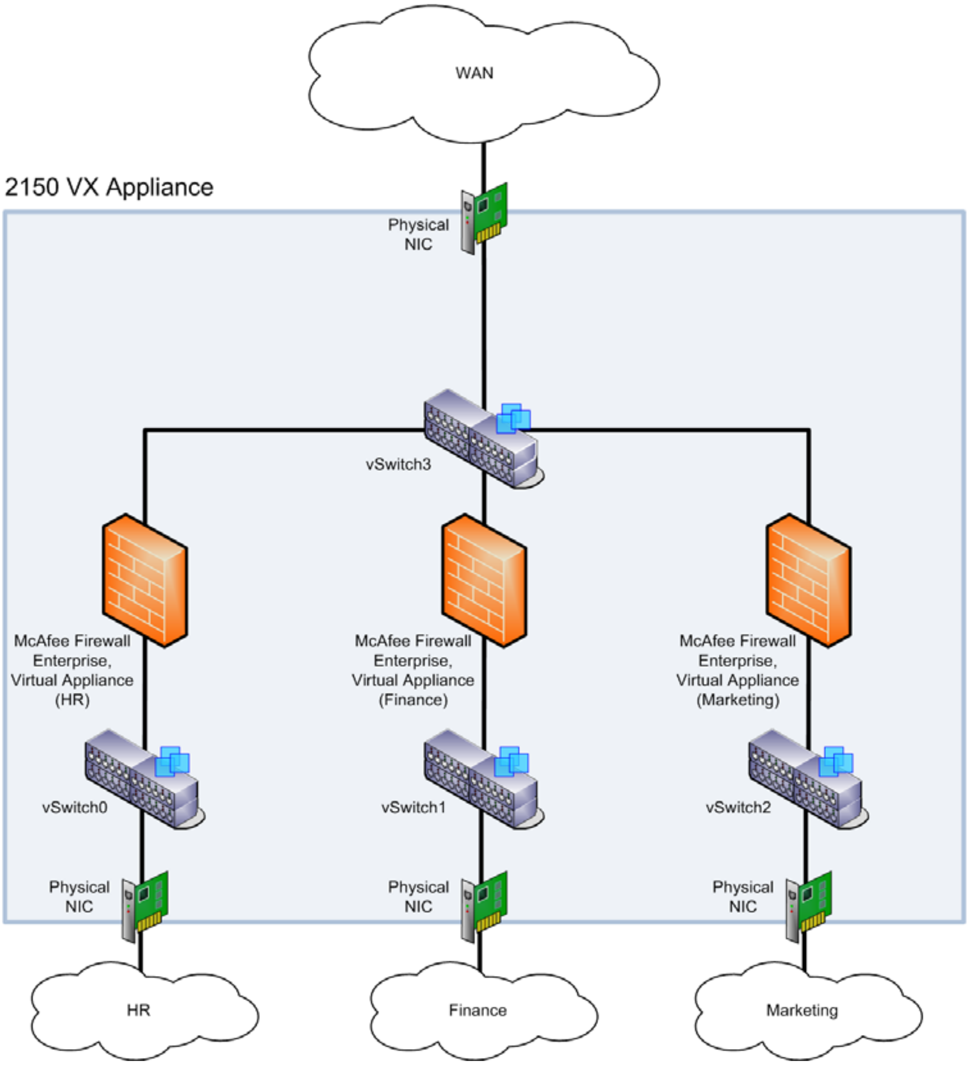
- Independent firewall management for each department (using the Firewall Enterprise Admin Console)
- Physical separation between department networks
- Reduced operating costs (a single 2150 VX appliance hosts the virtual firewalls)

Some alternate configuration options include:

- **VLANs** – Instead of dedicating a single physical NIC to connect each virtual firewall to the department networks, you can use VLANs to separate multiple networks on a single shared physical NIC. For example, if the HR, Finance, and Marketing networks are segmented by VLANs rather than physically, you can create a vSwitch with VLAN port groups and connect it to a single physical NIC.
- **High Availability** – If you purchased two 2150 VX appliances, you can configure virtual HA clusters across both appliances. See *Consolidated High Availability*.

A consolidated segmentation scenario is shown in Figure 1. In this scenario, the HR, Finance, and Marketing departments are each allocated a virtual firewall. While up to 32 virtual firewalls are supported, Figure 1 shows three to reduce complexity.

Figure 1 Firewall segmentation on a single 2150 VX appliance


WAN
2150 VX Appliance
Physical NIC
vSwitch3
McAfee Firewall Enterprise, Virtual Appliance (HR)
McAfee Firewall Enterprise, Virtual Appliance (Finance)
McAfee Firewall Enterprise, Virtual Appliance (Marketing)
vSwitch0
vSwitch1
vSwitch2
Physical NIC
Physical NIC
Physical NIC
HR
Finance
Marketing

McAfee Firewall Enterprise Control Center management

This scenario introduces Firewall Enterprise Control Center management to the *Consolidated segmentation* scenario. In this scenario, administrators centrally manage the virtual firewalls by connecting to the Control Center, Virtual Appliance.

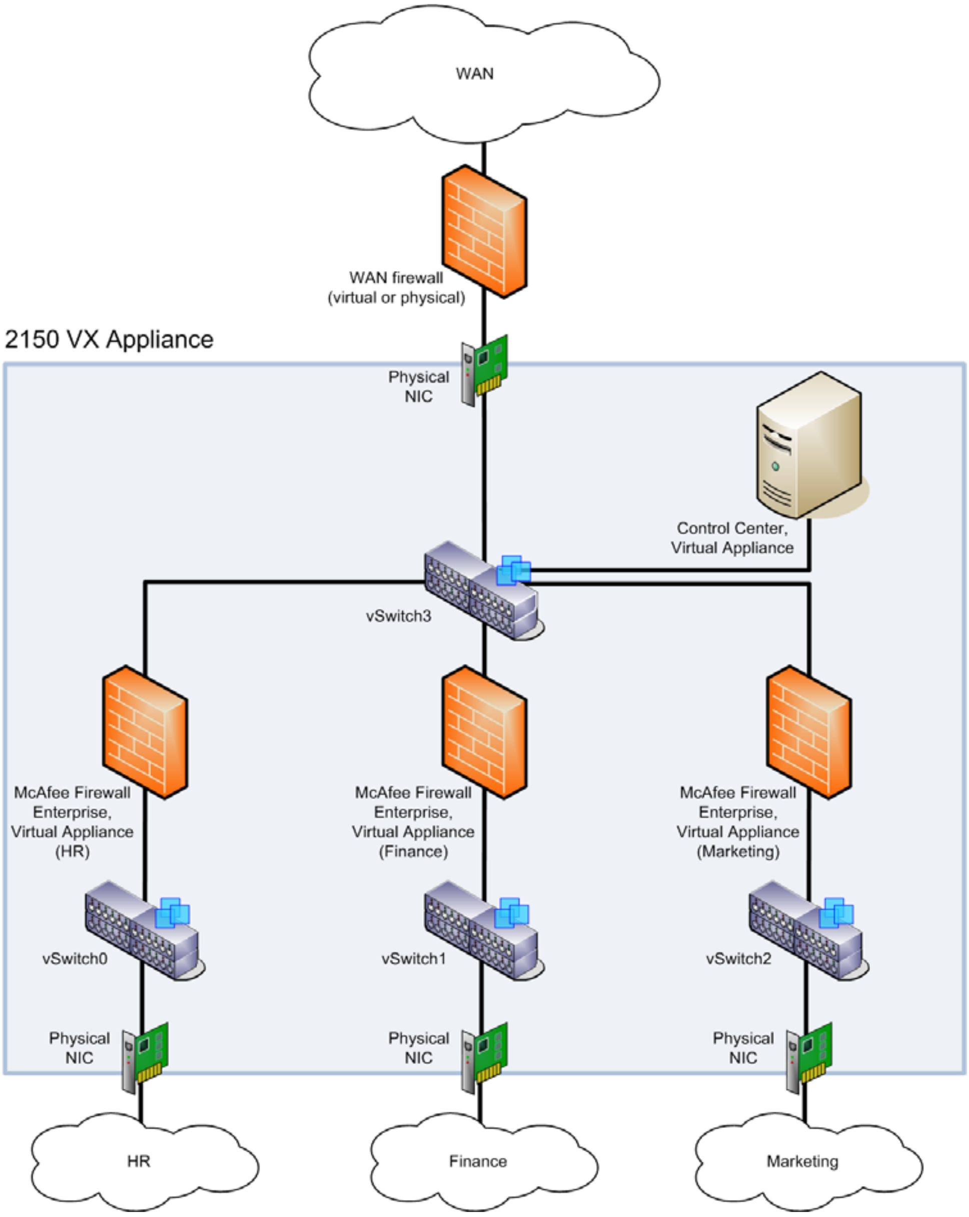
To use this management option, you must configure virtual networking so that the virtual Control Center has network connectivity to the:

- Virtual firewalls (required to manage them)
- Internet (required to maintain the Control Center, Virtual Appliance's license)

In the example shown in Figure 2, the Control Center, Virtual Appliance is connected to vSwitch3, which provides connectivity to the managed virtual firewalls and to the Internet.

The virtual Control Center must be protected by a firewall. In Figure 2, it is protected by the WAN firewall.

Figure 2 Control Center management on a 2150 VX appliance



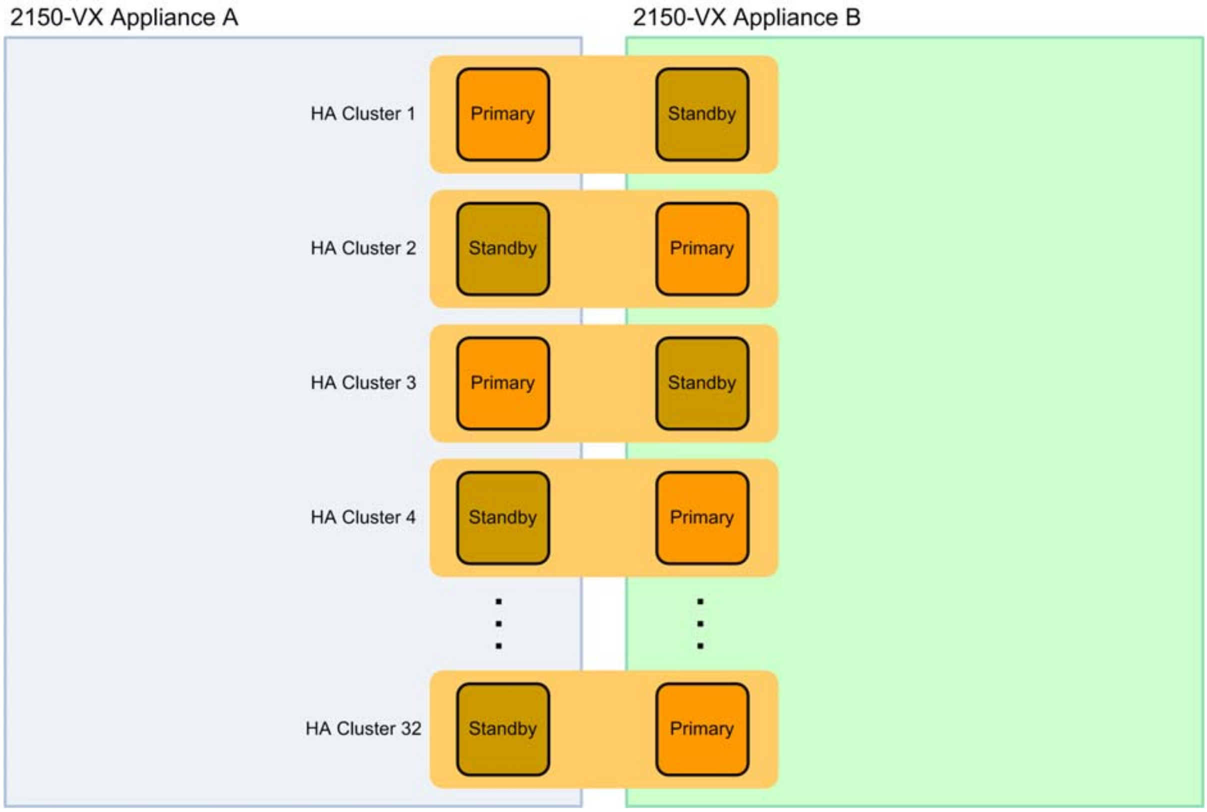
If you want to use Control Center centralized management while also restricting which firewalls administrators can manage, consider using Control Center configuration domains. For more information, see the *McAfee Firewall Enterprise Control Center (CommandCenter) Administration Guide*.

Consolidated High Availability

This scenario depicts primary/standby HA clusters created across two 2150 VX appliances. HA clusters provide the following benefits:

- Firewall consolidation and segmentation – See *Consolidated segmentation* on page 7.
- Failover – Redundancy protects against both hardware and software problems.
  - If there is a software problem on a primary virtual firewall, its standby virtual firewall on the second 2150 VX appliance takes over as the primary.
  - If one of the 2150 VX appliances experiences a hardware problem, all of its virtual firewalls fail over to the corresponding virtual firewalls on the second 2150 VX appliance.
- Increased performance – By configuring half of the primary virtual firewalls to run on the first 2150 VX appliance and the remaining half to run on the second 2150 VX appliance, each 2150 VX appliance effectively handles half of the load. See Table 3 below.

Figure 3 2150 VX HA concept



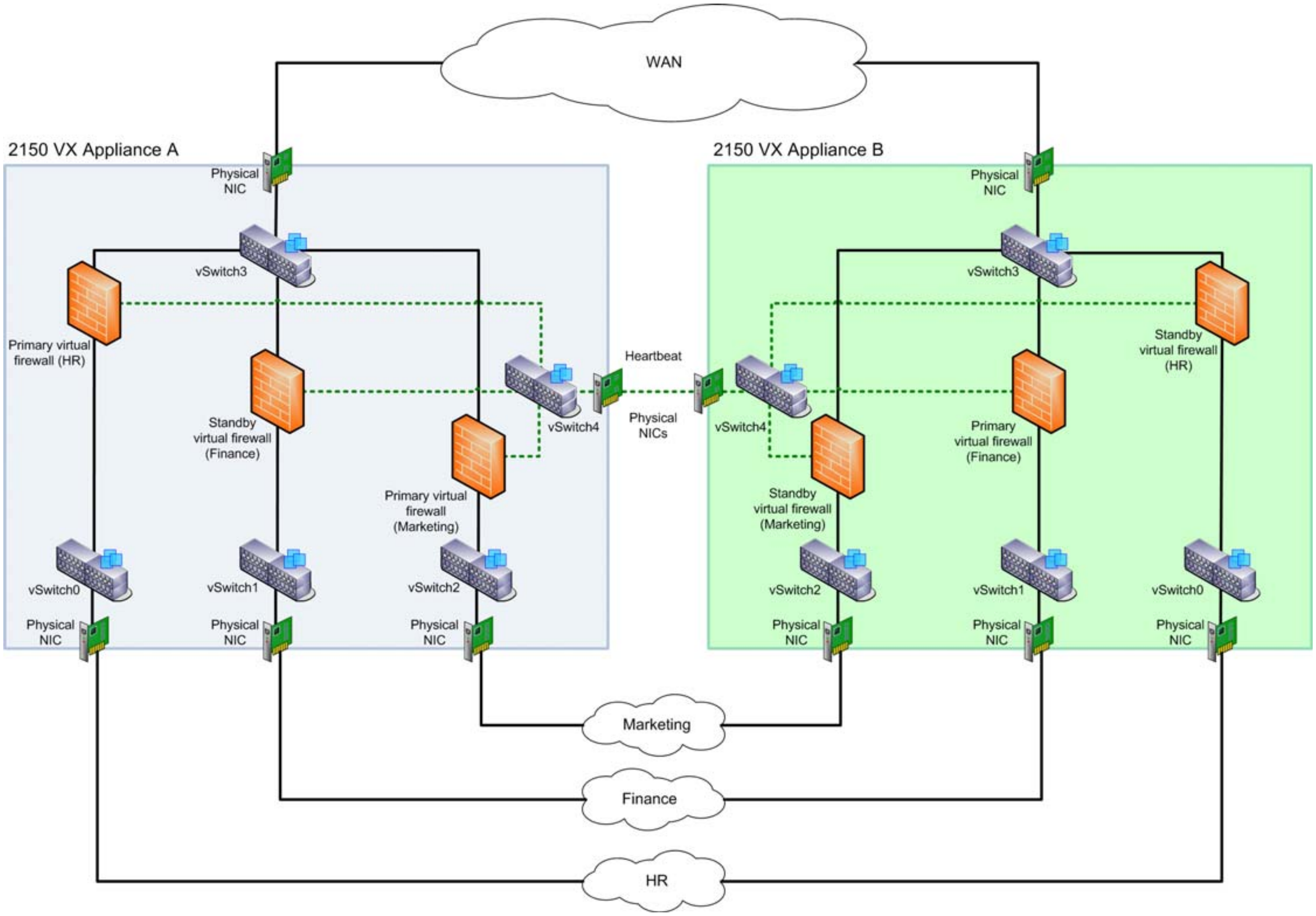
Network diagram

Figure 4 below shows three primary/standby HA clusters configured across two 2150 VX appliances (up to 32 clusters supported):

- **Marketing HA** – Primary virtual firewall configured on 2150 VX appliance A
- **Finance HA** – Primary virtual firewall configured on 2150 VX appliance B
- **HR HA** – Primary virtual firewall configured on 2150 VX appliance A

During normal operations (when all primary virtual firewalls are functional), 2150 VX appliance A processes traffic from the Marketing and HR networks, while 2150 VX appliance B processes traffic from the Finance network.

Figure 4 2150 VX HA network diagram


WAN
2150 VX Appliance A
2150 VX Appliance B
Physical NIC
vSwitch3
Primary virtual firewall (HR)
Standby virtual firewall (Finance)
Primary virtual firewall (Marketing)
vSwitch4
Heartbeat
Physical NICs
Standby virtual firewall (HR)
Primary virtual firewall (Finance)
Standby virtual firewall (Marketing)
vSwitch0
vSwitch1
vSwitch2
Marketing
Finance
HR

Two types of network connections are shown in Figure 4:

- Solid – Connections on which network traffic is passed
- Dotted – Heartbeat connections between HA cluster firewalls

Implementation requirements

To configure HA as depicted in this scenario, the following requirements must be met:

- All HA clusters must be cluster type primary/standby (Load-sharing is not supported).
- All normal HA configuration requirements must be met; refer to the high availability information in the *McAfee Firewall Enterprise (Sidewinder) Administration Guide*.
- Each 2150 VX appliance must meet the following virtual networking requirements:
  - Virtual network configuration must be consistent across both appliances.
  - A dedicated vSwitch must be configured to provide HA heartbeat connectivity for all HA clusters.
    - The vSwitch must have a unique VLAN port group for each HA cluster.
    - The vSwitch must be connected to the corresponding vSwitch on the other 2150 VX appliance by a physical NIC.

    Note: Each HA cluster heartbeat connection must be given a unique VLAN. Heartbeat connections for multiple HA clusters cannot share the same network space.

  For more information about virtual networking, see *About ESXi virtual networking* on page 17.

2 Set Up the 2150 VX Appliance

Contents

Verify materials

Make sure that you have all the necessary hardware, software, and documents needed to set up your McAfee Firewall Enterprise 2150 VX appliance.

Table 3 Materials included in your shipment

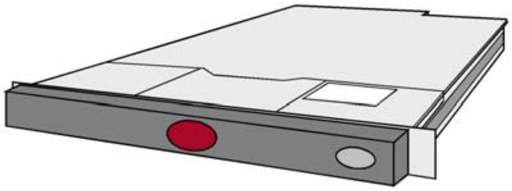
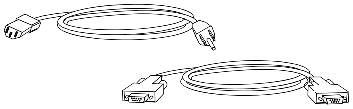
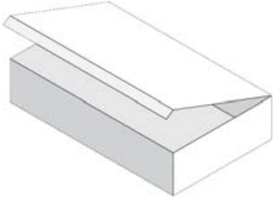
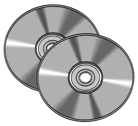
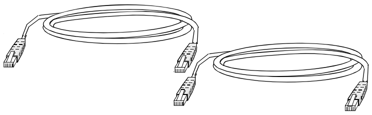
Hardware, software, and documents included in your shipment
 Appliance pre-loaded with ESXi, McAfee Firewall Enterprise, Virtual Appliances, and a McAfee Firewall Enterprise Control Center, Virtual Appliance
 Power cord and serial cable
 Rack Mount Kit
 McAfee Firewall Enterprise, Virtual Appliance USB Drive (Virtual appliance and management software) *McAfee Firewall Enterprise Control Center, Virtual Appliance USB Drive* (Virtual appliance and management software)
 Product Guide and *Activation Certificate*
 *VMware ESXi 3.5 Update 3 Installation CD* *VMware ESXi 3.5 Update 3 Patch CD*

Table 4 Materials you provide

Hardware	Component	Requirements
Management system (desktop or laptop) 	**OS**	MS Windows 2000 Workstation, 2000 Server, XP Professional, or Vista
	CPU	Intel (1 GHz minimum)
	Memory	512 MB minimum
	Drives	• 300 MB of available disk space • CD-ROM drive
	Display	1024 x 768 or higher
	NIC	Access to network hosting your firewall
	USB port	For USB drive
	Browser	• Internet Explorer 6 or later • Mozilla Firefox 1.0 or later
	**Network cables**	• At least two network cables for the 2150 VX appliance • One network cable for management system
	Monitor and Keyboard	VGA monitor and a USB keyboard to connect to the 2150 VX appliance

Set up the hardware

To set up your 2150 VX appliance and cables:

1. Determine the proper placement of your 2150 VX appliance based on the decisions you made in *Planning your deployment* on page 7.
2. Attach both power cords to the appliance and plug them into an electrical outlet.

   Note: Do not power on the firewall at this time.
3. Connect the Ethernet port labeled **Gb 1** to the network you will manage ESXi from.

   Note: This port should be connected to a private network that is accessible only to VMware administrators.
4. Connect a monitor and keyboard to the 2150 VX appliance.

Configure the ESXi environment

The ESXi management settings must be configured, the vSphere client installed, virtual networking configured, and NTP synchronized before your virtual machines can be deployed.

Configure the ESXi management settings

To configure the ESXi management settings:

1. Turn on the 2150 VX appliance. The appliance starts and a status screen appears.
2. Press **F2** to enter the configuration menu.
3. Select **Configure Root Password,** and set your administrative password.
4. Select **Configure Management Network,** and configure the ESXi management network interface.
5. When you are finished configuring the management network, press **Esc** until the Configure Management Network: Confirm screen appears.
6. Press **Y**. You return to the Customize System screen.
7. Press **Esc** to log out.

Install the ESXi management tools

Install the VMware Infrastructure Client on a Windows-based computer in the private management network that you connected to your 2150 VX appliance in *Set up the hardware* on page 14.

1. In a web browser, navigate to the URL shown on the 2150 VX appliance console.
2. Click **Download VMware Infrastructure Client**.
3. When the download is complete, install the VMware Infrastructure Client.

   Note: On the Custom Setup window of the installation wizard, select **Install VMware Infrastructure Update Service**.

4. Start the VMware Infrastructure Client, and connect to the 2150 VX appliance.

Activate your ESXi license

To license ESXi on your 2150 VX appliance, perform the following procedures:

- *Retrieve your ESXi serial number* on page 15
- *Generate the license file* on page 16
- *Add the license file to your 2150 VX appliance* on page 17

Retrieve your ESXi serial number

To retrieve your ESXi serial number:

1. In a web browser, navigate to https://www.vmware.com/vmwarestore/newstore/oem_login.jsp?Name=MCAFEE-AC.
2. Log in or register.

   Note: If you are already logged into the VMware web site, you are immediately taken to the VMware Partner Activation Code Registration page.

   - If you have an existing VMware account, enter your credentials, and click **Sign In**. The VMware Partner Activation Code Registration page appears.
   - If you do not have a VMware account, click **Register** under New Customers. The Register for Your VMware Product page appears.

Complete the Registration Information form with your information, and click **Continue**. The VMware Partner Activation Code Registration page appears.

3 In the **Partner Activation Code(s)** field, type the VMware activation code included on the *Activation Certificate*, and click **Continue**. The Add License Administrator page appears.

4 If desired, enter additional administrator e-mail addresses in the **License Administrator Email** field, and click **Continue**. The VMware Confirmation page appears.

5 Review the summary.

- If the information is incorrect, click **Back** to return to the previous page or click **Cancel** to return to the login page.
- If the information is correct, record the serial number, and click **Continue**.

  The Thank you page appears.

Generate the license file

To generate the license file:

1 In a web browser, navigate to www.vmware.com/support.

2 From the **Support Resources** menu, select **Product Licensing**. The VMware Product Licensing page appears.

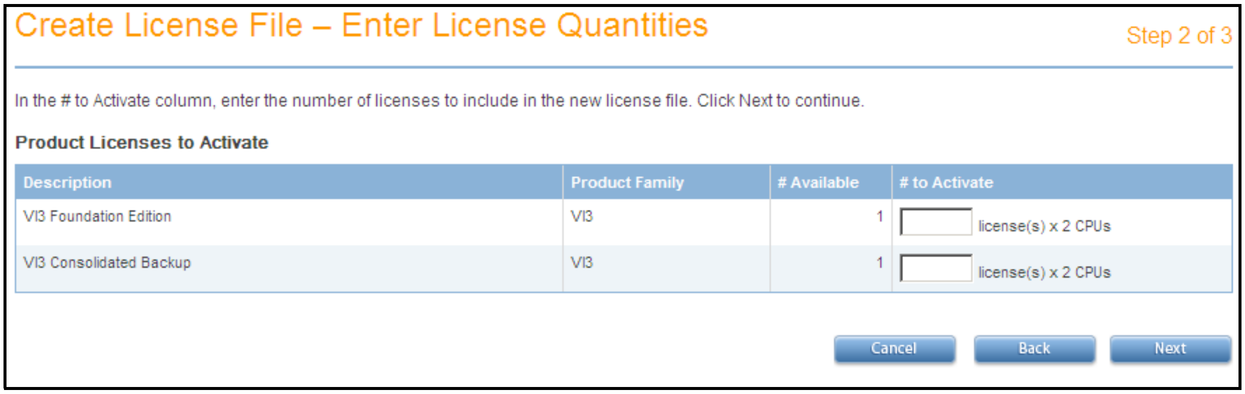
3 In the Manage Licenses with Activation Codes section, click **Manage Licenses**. The Manage Licenses page appears.

4 If you are prompted to log in, enter your credentials.

5 Click **Generate New License File**. The Create License File – Select Licensing Model page appears.

6 Select **Single Host**, and click **Next**. The Create License File – Enter License Quantities page appears.

Figure 5 Enter License Quantities page



Create License File – Enter License Quantities

Step 2 of 3

In the # to Activate column, enter the number of licenses to include in the new license file. Click Next to continue.

Product Licenses to Activate

Description	Product Family	# Available	# to Activate
VI3 Foundation Edition	VI3	1	☐ license(s) x 2 CPUs
VI3 Consolidated Backup	VI3	1	☐ license(s) x 2 CPUs

7 In the VI3 Foundation Edition or VI3 Standard Edition **# to Activate** field, type **1**, and click **Next**. The Create License File – Confirm page appears.

8 If desired, enter a comment in the **Comments** field, and click **Done**. The Create License File – Success page appears.

9 Obtain a copy of the license file using one of the following methods:

- To download the file, click **Download Now**.
- To have the file sent to you via e-mail, click **Send Email**.

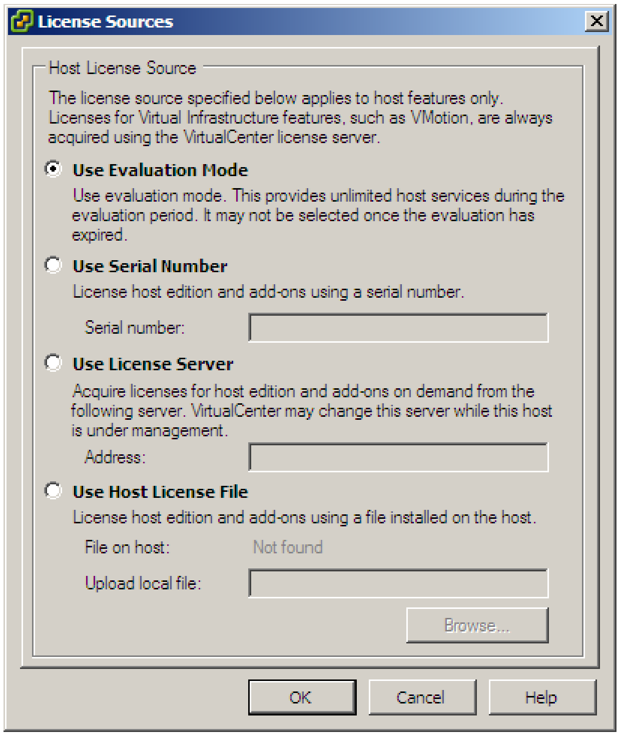
10 Click **Done**.

Add the license file to your 2150 VX appliance

To add the license file to your 2150 VX appliance:

1. Connect to your 2150 VX appliance using the VMware Infrastructure Client.
2. Click the **Configuration** tab, and click **Licensed Features**. The Licensed Features area appears in the right pane.
3. Next to License Source, click **Edit**. The License Sources window appears.

Figure 6 License Sources window



License Sources

Host License Source

The license source specified below applies to host features only. Licenses for Virtual Infrastructure features, such as VMotion, are always acquired using the VirtualCenter license server.

● **Use Evaluation Mode**

Use evaluation mode. This provides unlimited host services during the evaluation period. It may not be selected once the evaluation has expired.

○ **Use Serial Number**

License host edition and add-ons using a serial number.

Serial number:

○ **Use License Server**

Acquire licenses for host edition and add-ons on demand from the following server. VirtualCenter may change this server while this host is under management.

Address:

○ **Use Host License File**

License host edition and add-ons using a file installed on the host.

File on host: Not found

Upload local file:

4. Select **Use Host License File**.
5. Click **Browse**, select the license file that you obtained in *Generate the license file* on page 16,, and click **Open**. The full path of the license file populates the **Upload local file** field.
6. Click **OK**. The Disable ESX Server Evaluation window appears.
7. Click **OK**. The Release Current Licenses window appears.
8. Click **Yes**.

ESXi is now licensed on your 2150 VX appliance.

Configure ESXi virtual networking

Use the following sections to configure ESXi virtual networking based on the decisions you made in *Planning your deployment* on page 7:

- *About ESXi virtual networking* on page 17
- *Add virtual networks* on page 19

About ESXi virtual networking

To configure virtual networking:

1 In the VMware vSphere Client, select **Configuration > Networking**.

2 Select **Add Networking**. The Add Network wizard appears.

Use the wizard to configure the following virtual machine networking objects:

- **Virtual switch (vSwitch)** – A network object in ESXi that connects virtual machines to each other in the same manner that a physical switch links physical machines.
  - If the virtual machines connected to the vSwitch need to communicate with hosts on a physical network, you can join the vSwitch to the physical network by connecting it to an appropriate physical Ethernet adapter (also known as an uplink adapter).
  - If the virtual machines connected to the vSwitch only need to communicate with each other, you do not need to connect it to a physical Ethernet adapter.

  Note: By default, unconfigured virtual machines are connected to the Unconfigured vSwitch. Do not connect this vSwitch to a physical Ethernet adapter.

- **Port group** – A group of ports that provides a labeled, stable anchor point for virtual machines to connect to a vSwitch. Port groups include common parameters like VLAN tagging and bandwidth shaping. Multiple port groups can be assigned to a single vSwitch.

Tip: The Add Network Wizard always creates a new port group, but a new vSwitch may or may not be created depending on your choices.

Each McAfee Firewall Enterprise, Virtual Appliance has four network interfaces, each of which must be connected to an ESXi virtual switch (vSwitch) by mapping it to a port group. Note the following networking requirements:

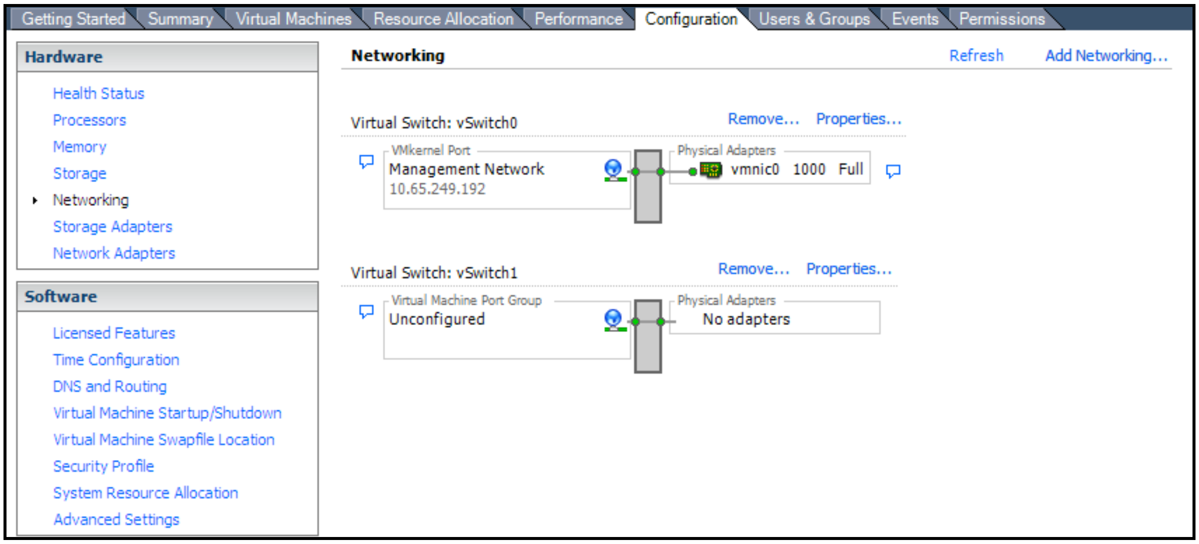
- Interface assignments on individual virtual firewalls cannot overlap; each interface must be assigned to a unique vSwitch. This rule applies only on a per-firewall basis; the virtual switches themselves may have multiple interfaces assigned to them. For example, you could configure five virtual firewalls, and on each configure one (and only one) DMZ interface, then assign those five DMZ interfaces to a single DMZ vSwitch.
- One virtual switch must be connected to a physical adapter on your 2150 VX appliance that provides Internet access. Internet connectivity is required to meet the license requirements of the virtual appliances.

Add virtual networks

To configure a new virtual network connection:

1 In the VMware Infrastructure Client, click the **Configuration** tab, and click **Networking**. The Networking area appears in the right pane.

Figure 7 Networking area



Virtual Switch: vSwitch0

VMkernel Port: Management Network, 10.65.249.192

Physical Adapters: vmnic0 1000 Full

Virtual Switch: vSwitch1

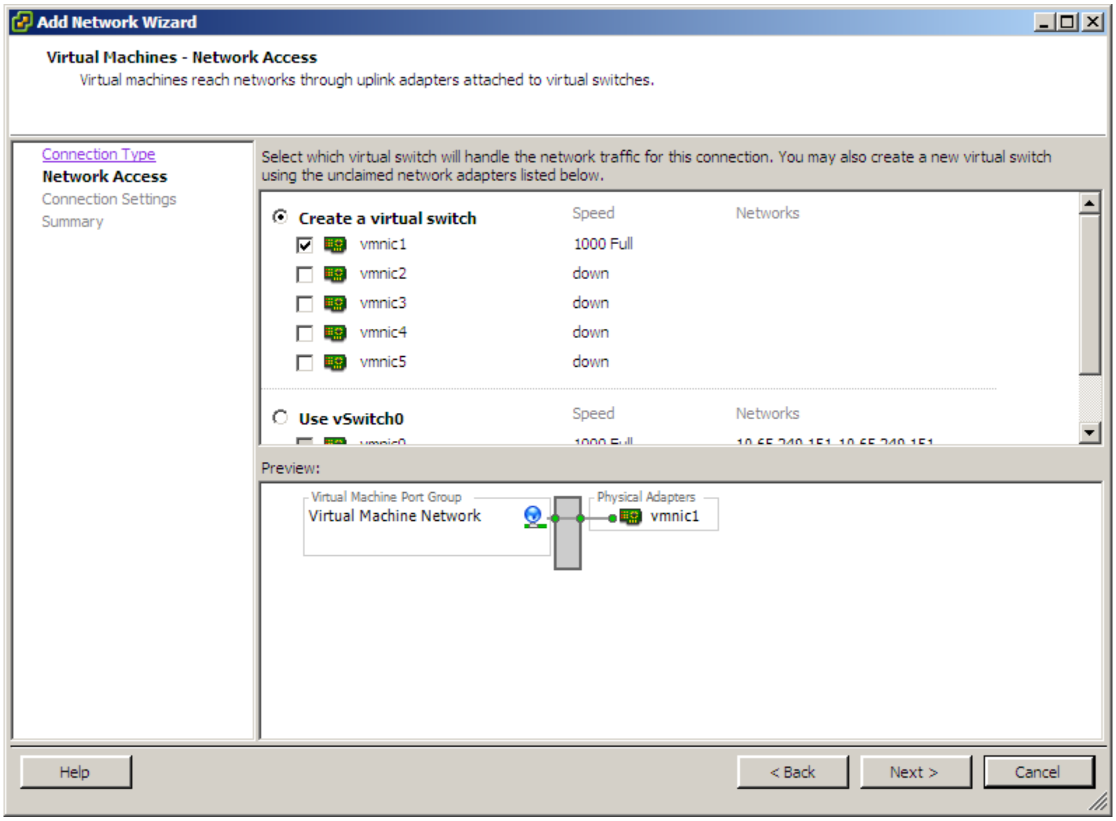
Virtual Machine Port Group: Unconfigured

Physical Adapters: No adapters

2 Click **Add Networking**. The Add Network Wizard window appears.

3 Select **Virtual Machine**, and click **Next**. The Network Access window appears.

Figure 8 Network Access window



Virtual Machines - Network Access

Virtual machines reach networks through uplink adapters attached to virtual switches.

Select which virtual switch will handle the network traffic for this connection. You may also create a new virtual switch using the unclaimed network adapters listed below.

● Create a virtual switch	Speed	Networks
☑ vmnic1	1000 Full	
□ vmnic2	down	
□ vmnic3	down	
□ vmnic4	down	
□ vmnic5	down	
○ Use vSwitch0	Speed	Networks
□ vmnic0	1000 Full	10.65.249.151-10.65.249.151

Virtual Machine Port Group: Virtual Machine Network

Physical Adapters: vmnic1

4 Select the virtual switch that will handle network traffic for this connection,, and click **Next**:

- If you need to create a new vSwitch, select **Create a virtual switch**. Enable or disable physical Ethernet adapters for this vSwitch as desired.
- If you want to assign this connection to an existing vSwitch, select it from the list.

The Connection Settings window appears.

5 In the **Port Group Properties** area, configure the following items, and click **Next**:.

- **Network Label** – Enter a name for this port group.
- **VLAN ID** – [Optional] To configure this port group to participate in VLAN tagging, enter a VLAN ID between 1–4095.

The Summary window appears.

6 Examine the Preview.

- If you are satisfied with your changes, click **Finish**.
- If you need to modify your changes, click **Back**.

The new connection configuration is complete.

Tip: To modify a vSwitch after it has been created, click **Properties** next to it.

Configure NTP

McAfee recommends configuring your 2150 VX appliance to synchronize its system clock with a time server using the Network Time Protocol (NTP).

Note: Because virtual appliance system clocks can also drift away from the ESXi system clock, McAfee recommends configuring NTP on your virtual firewalls and Control Center virtual appliance.

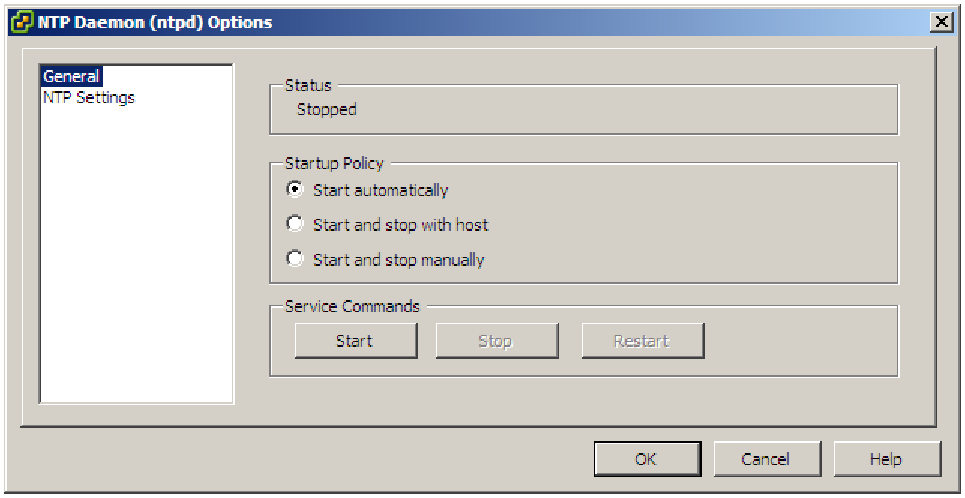
To configure NTP on your 2150 VX appliance:

1 In the VMware Infrastructure Client, click the **Configuration** tab, and click **Time Configuration**. The Time Configuration area appears in the right pane.

2 Click **Properties**. The Time Configuration window appears.

3 Click **Options**. The NTP Daemon (ntpd) Options window appears.

Figure 9 NTP Daemon (ntpd) Options window



NTP Daemon (ntpd) Options

General
NTP Settings

Status
Stopped

Startup Policy
● Start automatically
○ Start and stop with host
○ Start and stop manually

Service Commands

4 In the Service Commands area, click **Start**. The status changes to Running.

5 In the left pane, click **NTP settings**.

6 Add an NTP server.

- **a** Click **Add**. The Add NTP Server window appears.
- **b** Enter the host name or IP address of an NTP server, and click **OK**. The Add NTP Server window closes, and the server is added to the list of NTP servers.

If desired, repeat this step to add additional NTP servers.

7. Select **Restart NTP service to apply changes**, and click **OK**. The NTP Daemon (ntpd) Options window closes.
8. Click **OK** to close the Time Configuration window.

NTP is now configured on your 2150 VX appliance.

VMware upgrade with VMware tools

If you are upgrading your VMware environment to a version that is not included on the installation media McAfee provided, use the VMware tools and images to complete the upgrade.

For more information about upgrade path compatibility, see the VMware page at http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

Upgrade process overview

There are several upgrade paths available when upgrading your VMware ESXi software.

Use these high-level steps for an upgrade. For more information, refer to the VMware resources.

1. Go to the VMware support and downloads page: http://www.vmware.com/support/
2. Download the VMware upgrade documentation appropriate for your upgrade path.
3. Contact McAfee Technical Support for the necessary upgrade files.

   Note: An eUSB image of VMware 5.1 is available on the McAfee downloads page at http://www.mcafee.com/us/downloads. You will need your grant number.

4. Create backups of firewall and Control Center server configurations.

   Caution: The backups must be stored separately from the VMware host.

5. Halt and turn off the virtual machines.
6. Install the upgrade with the appropriate tool for your path.

Table 5

Upgrading to 4.x with vSphere CLI	Upgrading to 5.x with a USB drive
a Place the VMware host in maintenance mode. **b** Install the vSphere CLI .exe file. **c** Install the upgrade using the vSphere CLI.	**a** Image the USB drive. See KnowledgeBase article KB69115 for imaging instructions. **b** Restart the VMware host. **c** From the BIOS Boot Manager, install the uprade from the USB drive. **d** Remove the USB drive.

7. Restart the VMware host and restart the virtual appliances.
8. [For vSphere CLI upgrades only] Exit maintenance mode.
9. If you have any hard-coded ARP tables that include your firewall MACs, see if they need updating after the upgrade.

   Tip: The interface MAC addresses can change as a result of the upgrade process.

3 Configure the Control Center, Virtual Appliance

Contents

Configure the virtual Control Center

Use the following procedures to configure your McAfee Firewall Enterprise Control Center, Virtual Appliance:

- *Configure network mappings* on page 23
- *Perform initial configuration* on page 25

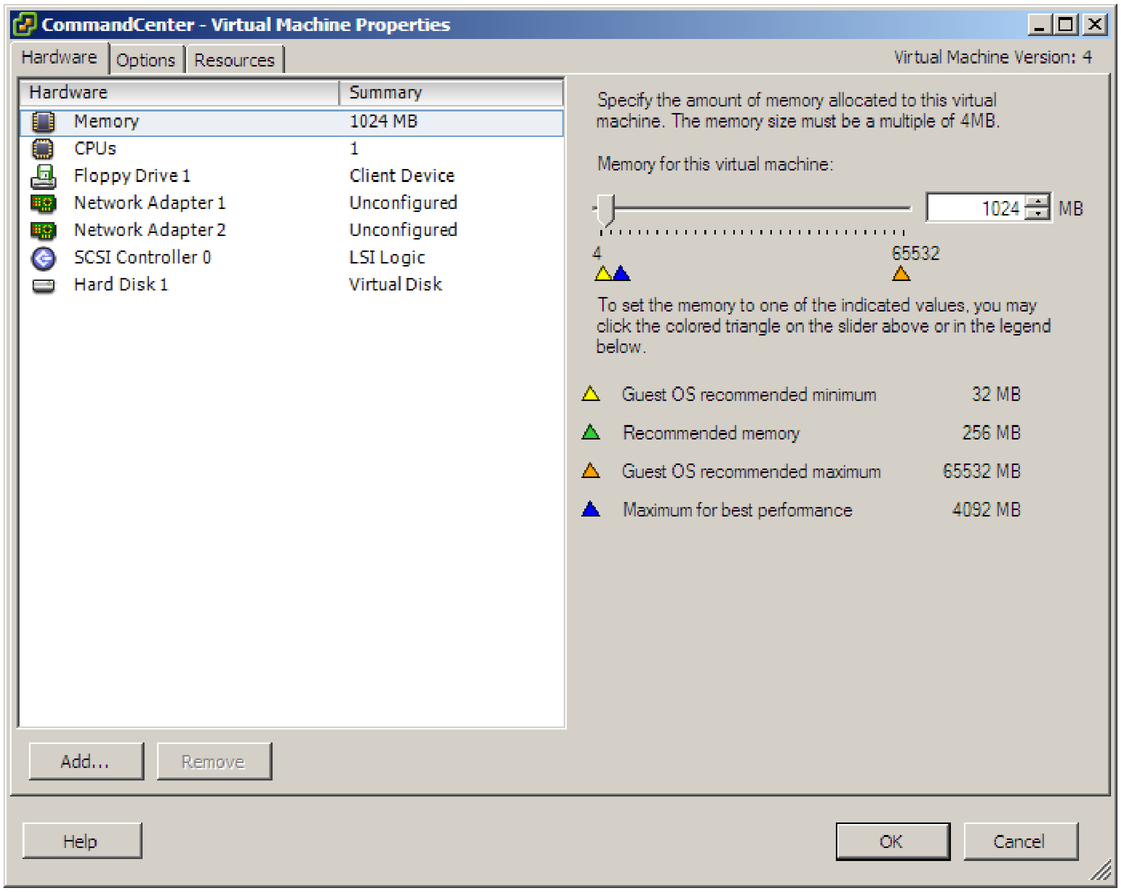
Note: If you do not want to use the Control Center virtual appliance to centrally manage your McAfee Firewall Enterprise, Virtual Appliances, skip this chapter and continue with *Chapter 4, Configure the McAfee Firewall Enterprise, Virtual Appliances*.

Configure network mappings

To configure network mappings for the virtual Control Center:

1. Select the virtual Control Center.
2. Click the **Getting Started** tab, and click **Edit virtual machine settings**. The Virtual Machine Properties window appears.

Figure 10 Virtual Machine Properties window



CommandCenter - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 4
Add...
Remove
Help
OK
Cancel

Hardware	Summary
Memory	1024 MB
CPUs	1
Floppy Drive 1	Client Device
Network Adapter 1	Unconfigured
Network Adapter 2	Unconfigured
SCSI Controller 0	LSI Logic
Hard Disk 1	Virtual Disk

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4MB.

Memory for this virtual machine: 1024 MB

4 △▲ 65532 △

To set the memory to one of the indicated values, you may click the colored triangle on the slider above or in the legend below.

△	Guest OS recommended minimum	32 MB
△	Recommended memory	256 MB
△	Guest OS recommended maximum	65532 MB
▲	Maximum for best performance	4092 MB

3 Map each of the virtual Control Center's network adapters to the appropriate virtual network.

a Refer to Table 6, and select the network adapter you want to configure.

Table 6 Network adapters

Virtual machine hardware device	Virtual Control Center NIC
Network Adapter 1	eth0
Network Adapter 2	eth1

b From the **Network label** drop-down list, select the appropriate port group.

Note: The port group you select for **Network Adapter 1** must provide Internet connectivity to allow the virtual Control Center to maintain a current license.

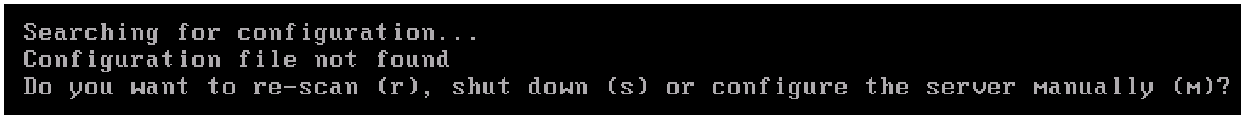
4 When you have configured all of the network adapters, click **OK**.

Perform initial configuration

To configure your virtual Control Center basic networking and administrator settings:

1. In the VMware Infrastructure Client, select the virtual Control Center.
2. On the Getting Started tab, click **Power on this virtual machine**. The virtual Control Center starts.
3. Click the **Console** tab. After startup is complete, the following message appears:

Figure 11 Searching for configuration



```
Searching for configuration...
Configuration file not found
Do you want to re-scan (r), shut down (s) or configure the server manually (m)?
```

4. Click inside the console window, and press **m**. The `Name of interface to configure` prompt appears.
5. Complete the initial configuration process using the information in Table 7.
   - Press **Enter** after each entry.
   - You will be asked to confirm your entries.

Table 7 Initial configuration responses

Prompt	Entry
Name of interface to configure	• To configure Network Adapter 1, type **eth0**. • To configure Network Adapter 2, type **eth1**.
IP address	Type an IP address that is appropriate for the network you mapped to this interface in *Configure network mappings* on page 23.
Network mask	Type a netmask that is appropriate for the IP address you specified
Do you wish to configure another interface	• If you do not want to configure the second interface, press **n**. • To configure the second interface, 1 press **y**. The `Name of interface to configure` prompt appears. 2 Specify configuration parameters for the second interface.
Gateway IP address	Type the IP address of the router that will handle packets destined for addresses not in your virtual Control Center routing table.
Enter this management server's host name (FQDN)	Type a host name for your virtual Control Center. Example: *controlcenter.example.com*
Enter the DNS server IP address	Type the IP address of a DNS server that is available on the configured interface(s).
Enter the domain name	Type the name of the domain your virtual Control Center is a member of. Example: *example.com*
Enter the SMTP server host name	Type the host name of an internal e-mail server. Example: *smtp.example.com*
Enter the CC Admin user name	• To use the default user name (ccadmin), press **Enter**. • To specify a custom user name, type the name.
A password will be assigned to the CC Admin user	Type a password for the CC admin user. Confirm the password.
Enter the dbuser PostgreSQL account password	Type a password for the dbuser user. Confirm the password.
Enter the sso UNIX account password	Type a password for the sso user. Confirm the password.
Enter the mgradmin UNIX account password	Type a password for the mgradmin user. Confirm the password.
Enter the ftp UNIX account password	Type a password for the ftp user. Confirm the password.

6 Configure your virtual Control Center's system clock settings.

When you have completed the `Do you want to specify an NTP server` prompt, you are finished with the initial configuration process.

The virtual Control Center uses your responses to perform its initial configuration. When it is finished, the login prompt appears.

Install the Control Center Client Suite

The following sections describe how to install the Control Center Client Suite:

- *About the Client Suite* on page 26
- *Verify Client Suite requirements* on page 26
- *Install the Client Suite* on page 27

About the Client Suite

The Client Suite is a collection of graphical user interface (GUI) tools that you use to manage your Control Center Management Server from a Windows system. Each of the tools is responsible for a set of tasks. All administrator accounts have access to all of the tools.

Table 8 Client Suite applications

Application	Description
Initialization Tool	Use to create the initial configuration file.
Administration Tool	Use to manage the Control Center administrative tasks, such as configuring users and roles, licensing, auditing, managing configuration domains, and configuring all system-wide configuration settings.
Configuration Tool	Use to manage the firewalls that are registered to the Control Center. Use this tool to configure and distribute security policies to your managed firewalls.
Reporting and Monitoring Tool	Use to centrally manage alerts and reports for your managed firewalls.
Software Updates Tool	Use to distribute software updates to your managed firewalls.

Verify Client Suite requirements

This section describes the hardware requirements for the Client Suite software that is installing and running administration software for your McAfee Firewall Enterprise Control Center Management Server. Verify that you have a system that meets or exceeds the requirements in Table 9.

Table 9 Minimum requirements for running Client Suite software

Component	Requirement
Operating system	Windows XP Professional with SP2 or later *or* Windows Vista
CPU	Intel Pentium 4 CPU (3.0 GHz or more)
Memory	2 GB recommended (1 GB minimum)
Drives	• 250 MB of available disk space • CD-ROM drive • USB flash drive (64 MB minimum)
Monitor	1024 x 768 or higher (1280 x 1024 is recommended)
Network interface card	Access to networks hosting your Management Servers

Install the Client Suite

To install the Control Center Client Suite on a Windows system:

1. Log into your Windows system as a user with administrative privileges.
2. [Conditional] If you have an earlier version of the Client Suite tools installed, uninstall any previous version of the Client Suite tools using the Windows Add/Remove Programs feature.
3. Insert the *Firewall Enterprise Virtual Appliance DVD* into the DVD drive.
4. In *McAfee_Firewall_Enterprise_Control_Center_40004_OVF_Virtual_Appliance.zip*, double-click the *setup.exe* file. The Welcome window appears.
5. Follow the on-screen instructions to complete the installation. Use the default settings.

The Client Suite software is now installed.

Connect using the Client Tools

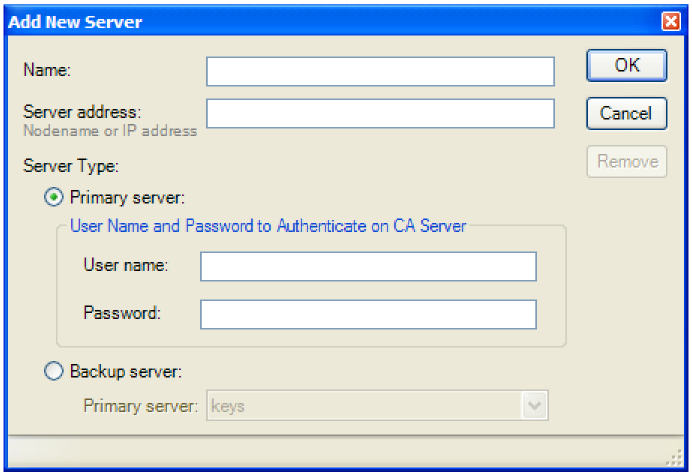
This procedure explains how to connect to your virtual Control Center using any of the Client Suite tools, and assumes that you are connecting to Control Center for the first time. If you have already configured Management Servers or certificates, select those objects in the appropriate fields.

From the Windows-based system that contains the Client Suite installation:

1. Select **Start > Programs > Secure Computing > CommandCenter 4.0**,, and select the appropriate tool.

   The Add New Server window appears.

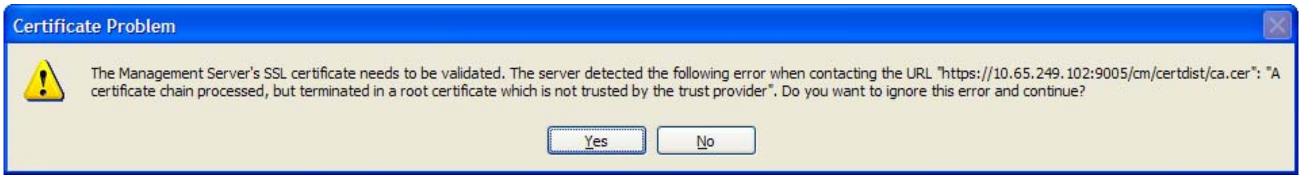
   Figure 12 Add New Server window



2. Enter the appropriate information:
   - In the **Name** field, enter a name that quickly identifies this Control Center Management Server.
   - In the **Server address** field, enter the host name or IP address of the Control Center Management Server.
   - Select **Primary server**, and complete the following fields with information appropriate for this Management Server:
     - In the **User name** field, specify a valid user name.
     - In the **Password** field, specify the appropriate password.

3 Click **OK**. The following message appears:

Figure 13 Certificate Problem message



Certificate Problem

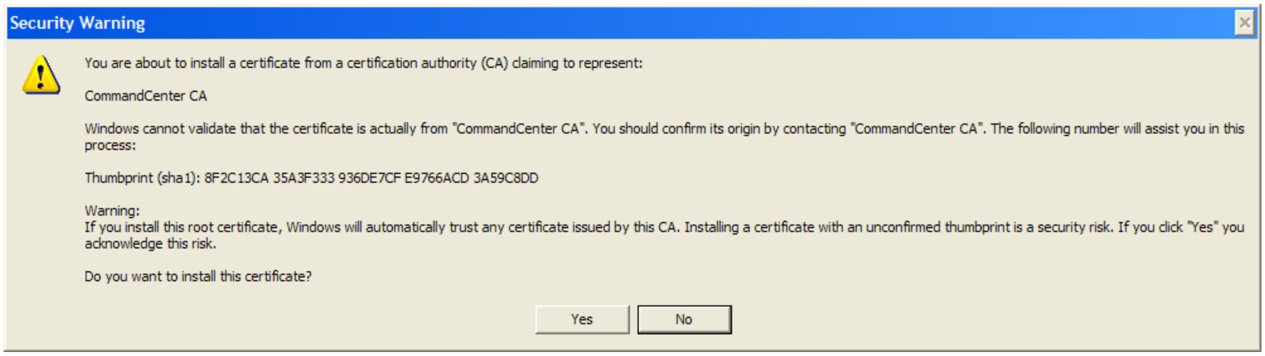
The Management Server's SSL certificate needs to be validated. The server detected the following error when contacting the URL "https://10.65.249.102:9005/cm/certdist/ca.cer": "A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider". Do you want to ignore this error and continue?

This message is expected. It is displayed because the application imports a non-Certificate Authority (CA) certificate before it imports the CA certificate of the Control Center Management Server. You can safely ignore this error.

4 Click **Yes**.

The Root Certificate Store message appears.

Figure 14 Root Certificate Store message



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

CommandCenter CA

Windows cannot validate that the certificate is actually from "CommandCenter CA". You should confirm its origin by contacting "CommandCenter CA". The following number will assist you in this process:

Thumbprint (sha1): 8F2C13CA 35A3F333 936DE7CF E9766ACD 3A59C8DD

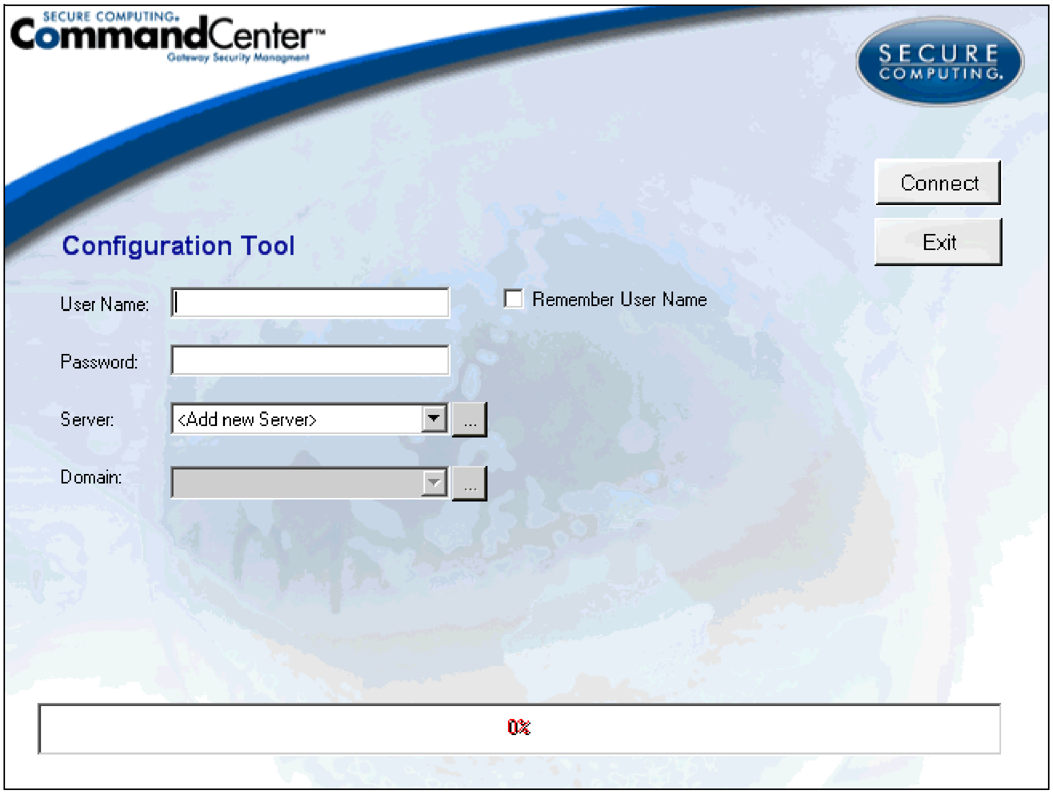
Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

5 Click **Yes**.

The main login window is displayed, and the newly created server is selected.

Figure 15 Main login window



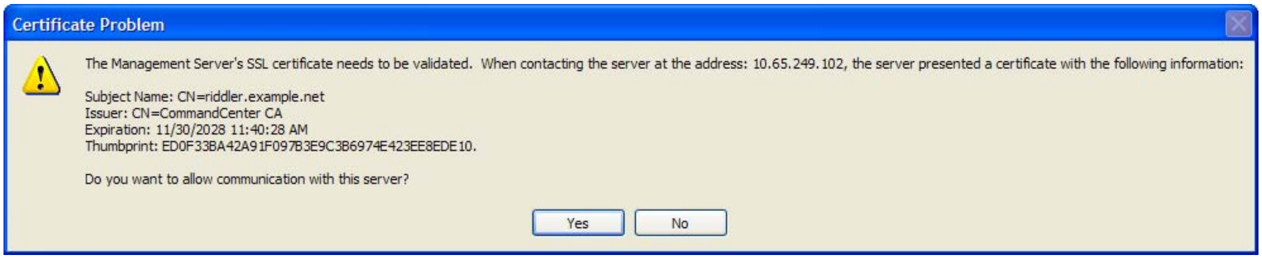
6 In the **User Name** field, specify a valid Control Center user name.

7 [Optional] Select **Remember User Name** to preserve the entered user name in the field on subsequent logins.

8 In the **Password** field, specify the corresponding password.

9 Click **Connect**. The following message appears:

Figure 16 Certificate validation message



Certificate Problem

The Management Server's SSL certificate needs to be validated. When contacting the server at the address: 10.65.249.102, the server presented a certificate with the following information:

Subject Name: CN=riddler.example.net
Issuer: CN=CommandCenter CA
Expiration: 11/30/2028 11:40:28 AM
Thumbprint: ED0F33BA42A91F097B3E9C3B6974E423EE8EDE10.

Do you want to allow communication with this server?

10 Click **Yes**.

You are now logged into the Control Center Management Server. You can start multiple Client Suite tools from the Tools menu in any tool without logging in again.

Note: If you attempt to log into a Management Server using Client Suite tools from a prior version, you will be prompted to update the Client Suite tools before proceeding.

Activate the license

The Control Center Management Server must be licensed before you can perform most administrative functions, such as registering firewalls, retrieving from and applying to firewalls, and performing software updates.

To license over the Internet, the Control Center Management Server establishes an HTTPS connection to the McAfee activation server on TCP port 443.

To activate the virtual Control Center license:

1. Using the Administration Tool, log on to the Control Center Management Server.
2. From the **System menu,** select **License**.
3. On the Server tab, in the **Serial Number** field, type the 16-character serial number located on the Activation Certificate or on your hardware platform.

   Do not change the default values for all other fields on this tab.
4. On the Contact tab, enter administrator information for this particular Management Server.
5. On the Company tab, enter your company information.
   - a On the Company Address tab, enter the company address.
   - b On the Billing Address tab, enter the billing address. If this information is the same as the company address information, click **Copy From Company Address**.
6. Click **Activate License**. The secure connection window appears.
7. Click **OK** to continue.

   The licensing information is sent to the activation server located at the URL defined in the Activation URL field. The activation server verifies the serial number and returns an activation key, which appears in the **Activation Key** field.
8. Click **OK** to close the form and save the licensing information.

Your license is now activated.

4 Configure the McAfee Firewall Enterprise, Virtual Appliances

Contents

Configure each McAfee Firewall Enterprise, Virtual Appliance

For each virtual firewall, perform the following tasks:

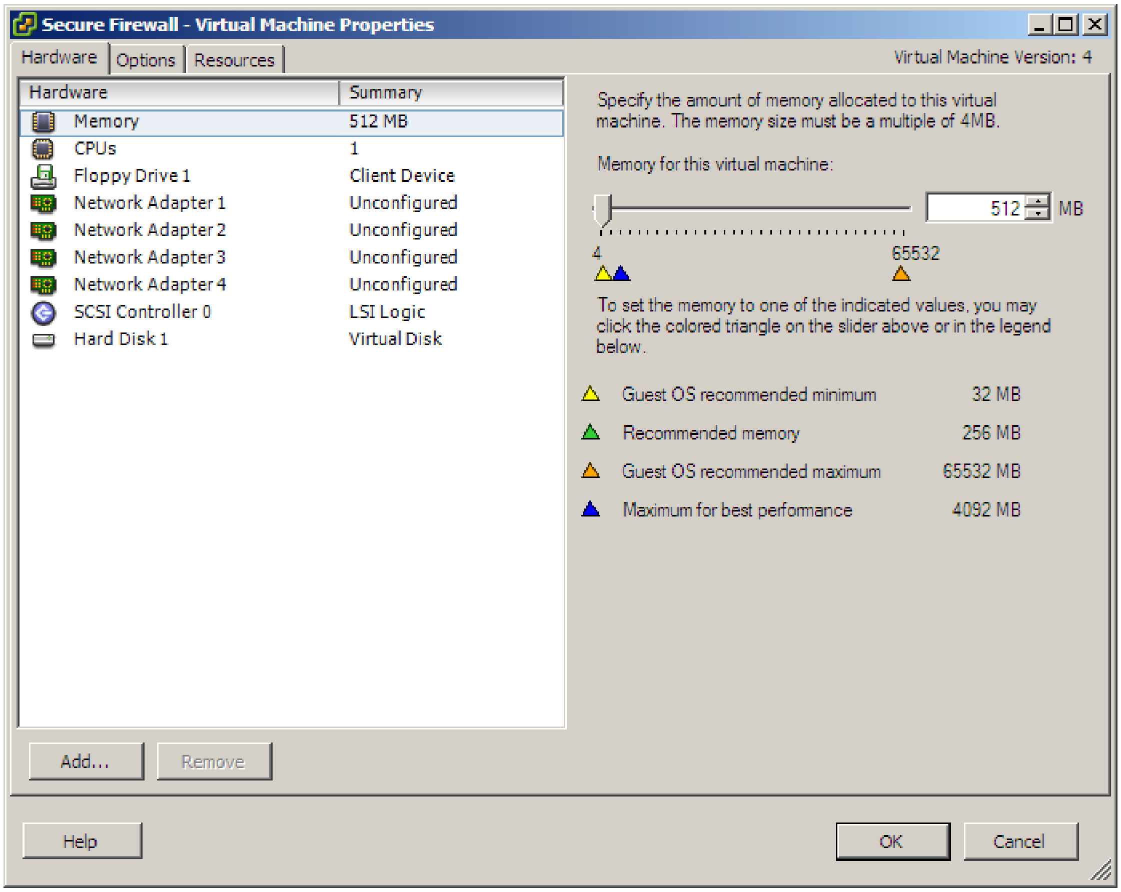
- *Configure network mappings* on page 31
- *Perform initial configuration* on page 33

Configure network mappings

To configure network mappings for a virtual firewall:

1. In VMware Infrastructure Client, connect to your 2150 VX appliance.
2. In the left pane, select the virtual firewall that you want to configure.
3. In the right pane, click the **Getting Started** tab,, and click **Edit virtual machine settings**. The Virtual Machine Properties window appears.

Figure 17 Virtual Machine Properties window



Secure Firewall - Virtual Machine Properties
Hardware
Options
Resources
Virtual Machine Version: 4
Add...
Remove
Help
OK
Cancel
MB
4
65532

Hardware	Summary
Memory	512 MB
CPUs	1
Floppy Drive 1	Client Device
Network Adapter 1	Unconfigured
Network Adapter 2	Unconfigured
Network Adapter 3	Unconfigured
Network Adapter 4	Unconfigured
SCSI Controller 0	LSI Logic
Hard Disk 1	Virtual Disk

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4MB.

Memory for this virtual machine: 512 MB

To set the memory to one of the indicated values, you may click the colored triangle on the slider above or in the legend below.

△	Guest OS recommended minimum	32 MB
△	Recommended memory	256 MB
△	Guest OS recommended maximum	65532 MB
▲	Maximum for best performance	4092 MB

4 Map each of the virtual firewall network adapters to the appropriate virtual network.

a Refer to Table 10, and select the network adapter you want to configure.

Table 10 Network adapters

Virtual machine hardware device	Virtual firewall NIC	Default burb
Network Adapter 1	em0	external
Network Adapter 2	em1	internal
Network Adapter 3	em2	*administrator configured*
Network Adapter 4	em3	*administrator configured*

b From the **Network label** drop-down list, select the appropriate port group.

Note: The port group you select for **Network Adapter 1** must provide Internet connectivity to allow the virtual firewall to maintain a current license.

5 [Conditional] If you plan to use features such as anti-virus scanning or Sendmail, increase the allocated memory to 1024 megabytes.

Note: Do not increase the number of virtual processors.

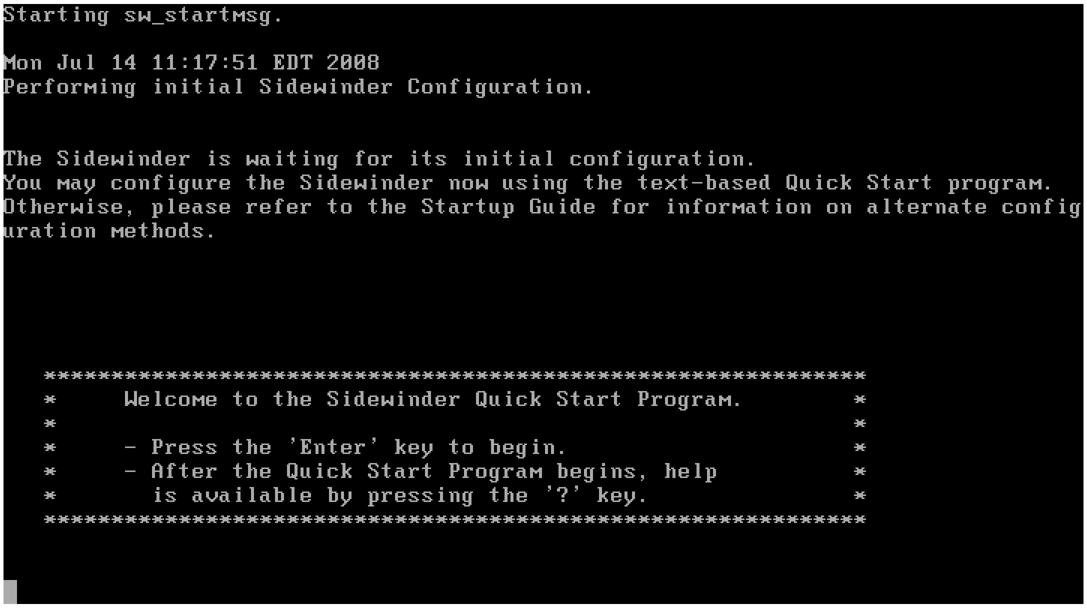
6 When you have configured all of the network adapters, click **OK**.

Perform initial configuration

To perform initial configuration of the virtual firewall:

1. In VMware Infrastructure Client, select the virtual firewall that you want to configure.
2. Click the **Getting Started** tab, and click **Power on this virtual machine**. The virtual firewall starts.
3. Click the **Console** tab. After startup is complete, the Sidewinder Quick Start Program appears.

Figure 18 Sidewinder Quick Start Program



```
Starting sw_startmsg.

Mon Jul 14 11:17:51 EDT 2008
Performing initial Sidewinder Configuration.


The Sidewinder is waiting for its initial configuration.
You may configure the Sidewinder now using the text-based Quick Start program.
Otherwise, please refer to the Startup Guide for information on alternate config
uration methods.






   *************************************************************
   *     Welcome to the Sidewinder Quick Start Program.        *
   *                                                           *
   *     - Press the 'Enter' key to begin.                     *
   *     - After the Quick Start Program begins, help          *
   *       is available by pressing the '?' key.               *
   *************************************************************
```

4. Click inside the console window, and press **Enter**. The Software License Agreement appears.
5. Read the Software License Agreement.

   Type **c**, and press **Enter** to advance the page. Continue until the text `Type Y to accept the license, N to decline the license, or R to redisplay the License` appears.
6. Press **y**, and press **Enter** to accept the license. The Serial number prompt appears.

7 Complete the Quick Start Program using the information in Table 11.

Press **Enter** after each entry.

Table 11 Quick Start Wizard responses

Prompt	Entry
Serial number	Type the serial number found on your *Activation Certificate*.
First Name through License Comments	Enter your registration information.
Do you want the Sidewinder to be managed by a CommandCenter server and use Rapid Deployment?	Press **n**.
Hostname	Type a host name for the virtual firewall. *Example: vfirewall.example.com*
Use DHCP for external interface?	Press **n**. Note: The McAfee Firewall Enterprise, Virtual Appliance does not support DHCP on the external interface at this time.
external IP	Type an IP address that is appropriate for the network you mapped to Network Adapter 1 in *Configure network mappings* on page 31.
external netmask	Type a netmask that is appropriate for the external IP address you specified above.
internal IP	Type an IP address that is appropriate for the network you mapped to Network Adapter 2 in *Configure network mappings* on page 31.
internal netmask	Type a netmask that is appropriate for the internal IP address you specified above.
external (internet) burb name	• To use the default name (external), press **Enter**. • To specify a custom name, type the name.
internal burb name	• To use the default name (internal), press **Enter**. • To specify a custom name, type the name.
Primary DNS IP	Type the IP address of a DNS server that is available on the external burb.
Secondary DNS IP	• If you do not want to specify a secondary DNS server, press **Enter**. • To specify a secondary DNS server, type the IP address of the server.
Default route	Type the IP address of the router that will handle packets destined for addresses not in your virtual appliance's routing table. Note: The default route you specify must provide Internet connectivity.
Internal mail host	Type a host name for an internal e-mail server. Example: *smtp.example.com*
Do you need an additional route for administrative or CommandCenter access?	Press **n**.
Username	Type a user name to create an administrative user.
Password	Type a password for the administrative user.
Administrator email address	• If you do not want to specify an e-mail address for the administrative account, press **Enter**. • To specify an e-mail address for the administrative account, type the address. A summary of your input appears.

8 Press **Enter**. The text `Press 'E' to edit or 'A' to apply the configuration` appears.

9 Complete the configuration:

- If you would like to make changes to the configuration, press **e**, and press **Enter**.
- If you are satisfied with the configuration summary, press **a**, and press **Enter**.

When you apply the configuration, the virtual firewall uses your responses to perform its initial configuration. When initial configuration is complete, the login prompt appears.

Install the McAfee Firewall Enterprise Admin Console

The McAfee Firewall Enterprise Admin Console is the graphical user interface (GUI) application used to manage your firewall from a Windows computer. The Admin Console is the primary user interface for the firewall.

Note: The Windows-based computer you install the Admin Console on must reside in the same network as the internal interfaces of your virtual firewalls.

To install the Admin Console on a Windows-based computer:

1. Insert the *McAfee Firewall Enterprise Virtual Appliance USB Drive* into one of your computer's USB ports.
2. Use Windows Explorer to view the contents of the USB drive, and extract the .zip file to your computer's hard drive.
3. Use Windows Explorer to view the contents of the folder you extracted in Step 2, and double-click the .exe file. The Welcome window appears.
4. Follow the on-screen instructions to complete the setup program. McAfee recommends using the default settings.

Tip: You should also install an SSH client on your computer. An SSH client can be used to provide secure command line access to the firewall.

Connect to the virtual firewalls using the Admin Console

Using the information you provided in the Quick Start Program, connect to your virtual firewalls. Perform these steps for each virtual firewall:

1. From the computer you installed the Admin Console on in *Install the McAfee Firewall Enterprise Admin Console*, select **Start > Programs > Secure Computing > Secure Firewall (Sidewinder) > Admin Console**.

   The Secure Firewall Admin Console appears.
2. Add a firewall to the Admin Console tree.
   a. On the toolbar, click **New Firewall**. The Add Firewall window appears.
   b. Enter the firewall name and IP address,, and click **Add**.
3. In the left pane, select your firewall icon. In the right pane, click **Connect**.

   Tip: If a message appears stating "Failed to connect to SSL server," the firewall may not have finished rebooting. Try connecting again in a few minutes.
4. Enter the administrator user name and click **OK**.
5. Enter the password and click **Enter**.

   A Feature Notification window appears listing the features that are licensed on your firewall.

   Note: If a message appears stating "The SecureOS will expire in approximately 7 day(s)," the license was not automatically activated and you have a trial license. You must activate the license manually before the trial license expires. See *Manually activate a McAfee Firewall Enterprise license* on page 36 for instructions.
6. Click **Close**.

You are connected to your virtual firewall.

Manually activate a McAfee Firewall Enterprise license

The McAfee Firewall Enterprise license automatically activates after configuration. If your license did not auto-activate, the virtual appliance will operate for seven days with a trial license. These features are licensed during the trial period:

- SecureOS
- Support
- VPN
- Failover
- Strong Cryptography

Note: Your virtual firewall must have Internet access to activate its license.

To activate a virtual firewall license:

1. On your Activation Certificate, locate the serial number for your firewall.
2. In the Admin Console, select **Maintenance > License**. The License window appears.
3. Click the **Contact** tab and enter your company contact information.
4. Click the **Company** tab and enter your company information.
5. Click the **Firewall** tab and enter the firewall information:
   - a In the **Serial Number** field, type the 16-digit alpha-numeric serial number for this firewall.
   - b In the **Firewall ID** field, accept the default. Do not change the Firewall ID unless instructed by Technical Support.
6. Click **Activate Firewall**. The license information is sent to the McAfee licensing website using an encrypted HTTPS session.

   If the data is complete, the request is granted and a new activation key is written to the **Activation Key** field. The Current Features list updates with the new license information.

Your firewall software and any features you licensed are activated.

- If you intend to manage this virtual firewall with the Admin Console, you have finished the set up process.
- If you intend to manage this virtual firewall using the virtual Control Center, continue with *Chapter 5, Register Virtual Firewalls to the Virtual Control Center*.

5 Register Virtual Firewalls to the Virtual Control Center

Contents

About McAfee Firewall Enterprise Control Center management

The virtual Control Center allows you to centrally manage multiple McAfee Firewall Enterprise appliances, whether they are physical or virtual. This chapter contains instructions on configuring the virtual Control Center to manage the virtual firewalls that are hosted by your 2150 VX appliance:

- *Register each firewall to the virtual Control Center* on page 37
- *Add each firewall to the virtual Control Center* on page 38

Register each firewall to the virtual Control Center

To register your virtual firewalls to your virtual Control Center, perform these steps on each virtual firewall:

1. Using the McAfee Firewall Enterprise Admin Console, connect to the virtual firewall that you want to register.
2. Select **Maintenance > CommandCenter Registration**.
3. Specify the host name and IP address of the virtual Control Center.
4. [Optional] If you are using a High Availability Control Center configuration, click **Configure backup server**.
   - In the **Backup Server Name** field, specify the host name of the Management Server that is acting as a backup to the active Management Server.
   - In the **IP Address field**, specify the IP address of the Management Server that is acting as a backup to the active Management Server.
5. Click **Register with the CommandCenter Now**.
6. An authentication window is displayed.
7. Enter the Control Center administrator user name and password, and click **OK**.

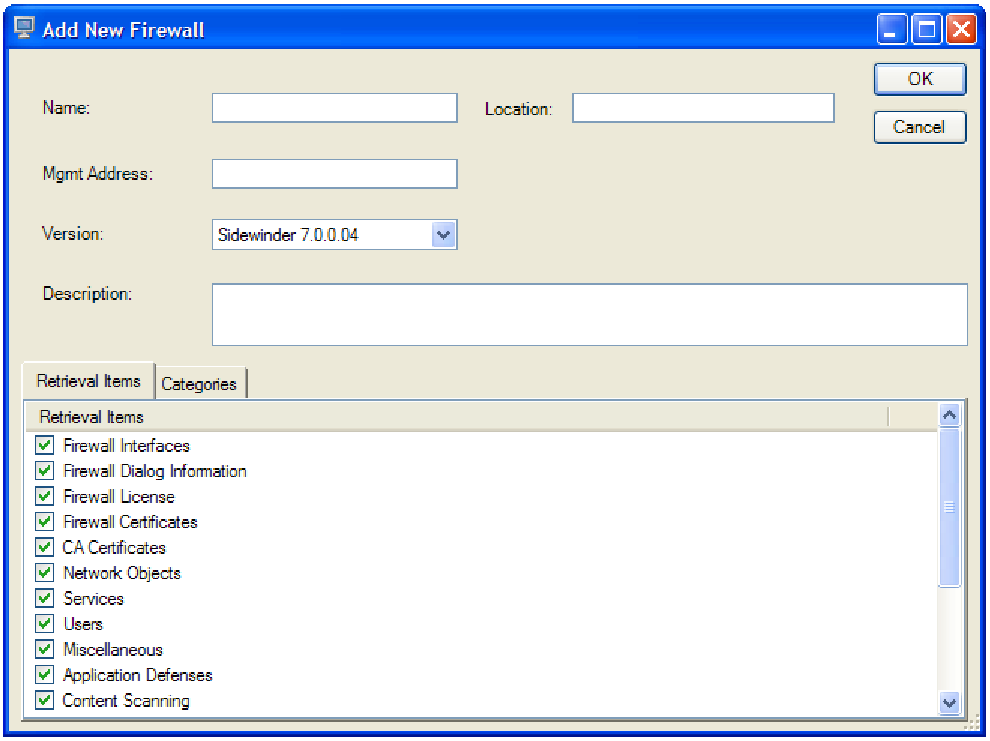
Repeat these steps to register all of the virtual firewalls to the virtual Control Center.

Add each firewall to the virtual Control Center

To add each virtual firewall to the virtual Control Center, perform these steps once for each virtual firewall:

1. Using the CommandCenter Configuration Tool, connect to your virtual Control Center.
2. Select the **Firewalls** group bar and perform one of the following steps:
   - **Standalone firewall** – If you are registering a *standalone* firewall, right-click **Firewalls** and click **Add Object**. The Add New Firewall window appears.

Figure 19 Add New Firewall window



Version: Sidewinder 7.0.0.04

Retrieval Items

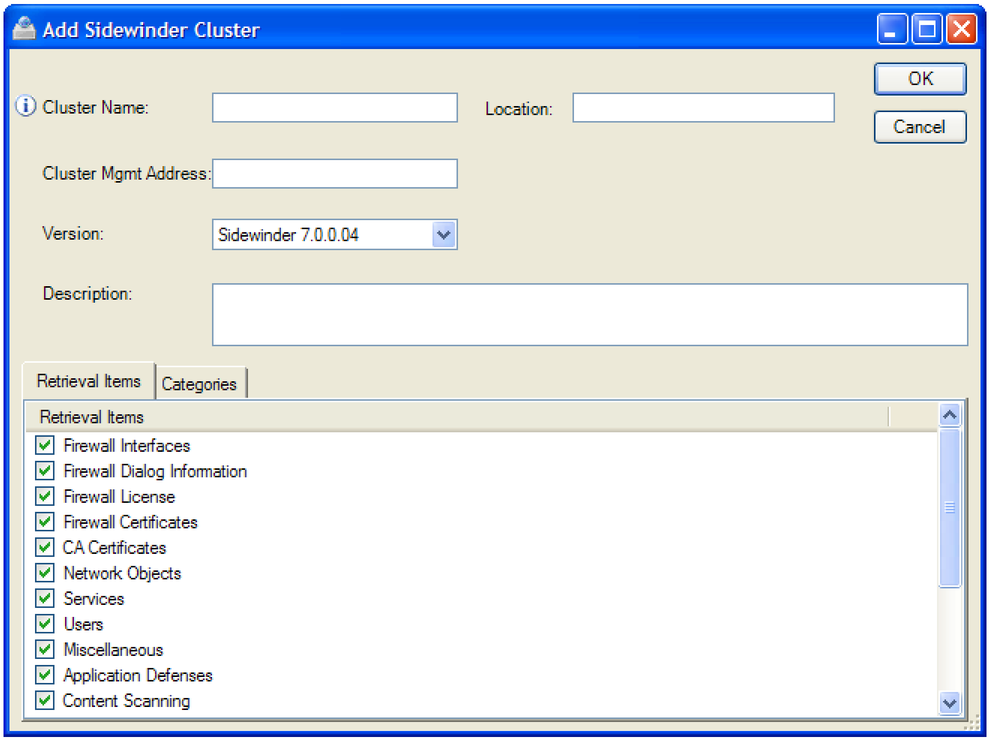
- ☑ Firewall Interfaces
- ☑ Firewall Dialog Information
- ☑ Firewall License
- ☑ Firewall Certificates
- ☑ CA Certificates
- ☑ Network Objects
- ☑ Services
- ☑ Users
- ☑ Miscellaneous
- ☑ Application Defenses
- ☑ Content Scanning

Specify the required information about the firewall:

- **Name** – Specify the name of the firewall. This is either the DNS name of the firewall or a user-specified name. Node names can be expressed in multiple parts and contain any sequence of letters and numbers, but they cannot begin with a number or contain most punctuation characters.
- **Mgmt Address** – Specify the firewall IP address that will be used for communication with your Control Center Management Sever.
- **Version** – Select the firewall's software version.

- **Cluster** – If you are registering a *cluster*, right-click **Clusters** and click **Add Object**. The Add Sidewinder Cluster window appears.

  Figure 20 Add Sidewinder Cluster window

  Add Sidewinder Cluster

  Cluster Name:

  Location:

  Cluster Mgmt Address:

  Version: Sidewinder 7.0.0.04

  Description:

  Retrieval Items

  ☑ Firewall Interfaces
  ☑ Firewall Dialog Information
  ☑ Firewall License
  ☑ Firewall Certificates
  ☑ CA Certificates
  ☑ Network Objects
  ☑ Services
  ☑ Users
  ☑ Miscellaneous
  ☑ Application Defenses
  ☑ Content Scanning

  Specify the required information about the cluster:

  - **Cluster Name** – Specify the name of the cluster. You can use any string of characters *except* for the FQDN of one of the cluster member nodes.
  - **Cluster Mgmt Address** – Specify the cluster IP address that will be used for communication with your Control Center Management Sever.
  - **Version** – Select the cluster software version.

3 On the Retrieval Items tab, right-click and select **Unselect All.** This saves time during an initial firewall registration by instructing the Control Center to establish connectivity without passing policy information.

4 Click **OK**. The Control Center attempts to connect to the firewall.

5 Verify communication between the firewall and the Management Server:

   a From the **Reports** menu, select **Firewall Status**.

   b Verify that a green light appears next to the firewall.

6 After a connection has been established, expand the **Firewalls** node or the **Clusters** node, depending on the object you are configuring.

7 Perform the following steps to retrieve the necessary objects:

a Right-click the firewall that you have just added and select **Retrieve Firewall Objects**. The Firewall Retrieval Options window is displayed.

b In the Retrieval Item Description column heading, right-click and select **Select All.**

Note: If you previously retrieved items from this firewall, consider clearing some of the checkboxes, such as rules, to avoid creating duplicates. McAfee does not recommend performing multiple retrievals of the same objects.

c Click **OK**. A system update message is displayed.

d Click **Yes**.

The Control Center initiates a connection with the firewall and retrieves the selected items.

After the virtual Control Center successfully connects to the firewall and retrieves the selected items, you can manage policy for that firewall.

6 Re-imaging

You can re-install a single virtual appliance or re-image the S7032 appliance.

Contents

Re-install a single virtual appliance

To re-install a single Firewall Enterprise, Virtual Appliance or Firewall Enterprise Control Center, Virtual Appliance, perform the following procedures:

- *Delete a virtual appliance* on page 41
- *Import a virtual appliance* on page 41

Delete a virtual appliance

To delete a virtual appliance:

1. Connect to your 2150 VX appliance using the VMware Infrastructure Client.
2. Click the **Virtual Machines** tab.
3. If the virtual appliance that you want to delete is powered on, right-click it in the list and select **Power Off**.
4. To delete the virtual appliance, right-click it and select **Delete from Disk**. A confirmation window appears.
5. Click **Yes**. The virtual appliance is deleted.

Import a virtual appliance

To load a single virtual appliance:

1. Move the virtual appliance onto the hard drive of your Windows-based client computer.
   - a Insert the appropriate USB drive.
   - b Extract the appliance file to your computer's hard drive.
2. Connect to your 2150 VX appliance using the VMware Infrastructure Client.
3. Click the **Getting Started** tab,, and click **Import a virtual appliance**. The Import Virtual Appliance Wizard appears.
4. Select the virtual appliance:
   - a Select **Import from file.**
   - b Click **Browse** to select the .ovf virtual appliance file you extracted in Step 1.
   - c Click **Next**. The Virtual Appliance Details window appears.
5. Click **Next**. The Name and Location window appears.
6. Enter a name for the virtual appliance, and click **Next**. The Network Mapping window appears.
7. From the drop-down list, select **Unconfigured**, and click **Next**. The Ready to Complete window appears.

8 Review the summary.

- If you are satisfied that the summary is correct, click **Finish**.
- If you need to make any changes, click **Back**.

When you click **Finish**, the virtual appliance uploads to your 2150 VX appliance.

When the upload is complete, configure the virtual appliance:

- If you imported a McAfee Firewall Enterprise Control Center, Virtual Appliance, see *Chapter 3, Configure the Control Center, Virtual Appliance*.
- If you imported a McAfee Firewall Enterprise, Virtual Appliance, see *Chapter 4, Configure the McAfee Firewall Enterprise, Virtual Appliances*.

Re-image your McAfee Firewall Enterprise 2150 VX appliance

To re-image your 2150 VX appliance, perform the following procedures:

- *Install VMware ESXi* on page 42
- *Configure the ESXi management settings* on page 43
- *Create a new isolated port group* on page 43
- *Install ESXi software updates* on page 44
- *Import multiple virtual appliances* on page 45

Install VMware ESXi

1 Connect your 2150 VX appliance to a monitor and keyboard.

2 Insert the *VMware ESXi 3.5 Update 3 Installation CD* into the CD drive.

3 When the `F11 = Boot menu` line appears in the upper right corner of your screen, press **F11**. The boot menu appears.

4 Select **CD-ROM drive**, and press **Enter**.

Your 2150 VX appliance boots from the *VMware ESXi 3.5 Update 3 Installation CD* and a Welcome screen appears.

5 Press **Enter** to continue with the installation.

6 Read the end user license agreement and accept it by pressing **F11**. The Select a Disk screen appears.

7 Select the disk on which to install VMware ESXi, and press **Enter**.

If the disk you selected contains data, the Confirm Disk Selection screen appears, warning that the selected disk is about to be overwritten. Confirm the disk choice or change the target disk:

- To change the target disk, press **Backspace**, and make a new selection.
- To confirm your disk selection, press **Enter**. The Confirm Install screen appears.

8 Press **F11** to start the installation.

When the installation is complete, the Installation Complete screen appears.

9 Remove the installation CD from the CD drive.

10 Press **Enter** to restart your 2150 VX appliance.

VMware ESXi is now installed.

Configure the ESXi management settings

To configure the ESXi management settings:

1. Turn on the 2150 VX appliance. The appliance starts and a status screen appears.
2. Press **F2** to enter the configuration menu.
3. Select **Configure Root Password** to set your administrative password.
4. Select **Configure Management Network** to configure the ESXi management network interface.
5. When you are finished configuring the management network, press **Esc** until the Configure Management Network: Confirm screen appears.
6. Press **Y**. You return to the Customize System screen.
7. Press **Esc** to log out.

Continue with *Create a new isolated port group*.

Create a new isolated port group

Create a new port group that is not connected to a physical interface. This port group will be referenced by unconfigured virtual appliances.

1. Connect to your 2150 VX appliance using the VMware Infrastructure Client.
2. Click the **Configuration** tab, and click **Networking**. The Networking area appears in the right pane.
3. Click **Add Networking**. The Add Network Wizard Connection Type window appears.
4. Select **Virtual Machine**, and click **Next**. The Network Access window appears.
5. Create a virtual switch that is not connected to any physical network adapters.
   a. Select **Create a virtual switch**.
   b. Clear the check boxes next to the physical network adapters (vmnics).
   c. Click **Next**.

   The Connection Settings window appears.
6. In the **Network Label** field, type **Unconfigured**, and click **Next**. The Summary window appears.

   Note: The port group must be named **Unconfigured** because it is referenced in the batch file used in “Import multiple virtual appliances” on page 20.
7. Click **Finish**. The Add Network Wizard closes.
8. Increase the number of ports on vSwitch1 (the vSwitch you just created).
   a. Next to vSwitch1, click **Properties**. The vSwitch1 Properties window appears.
   b. Select **vSwitch**, and click **Edit**. A pop-up window appears.
   c. From the **Number of Ports** drop-down list, select **248**.
   d. Click **OK**. A confirmation window appears.
   e. Click **OK**. The pop-up window closes.
   f. Click **Close**. The vSwitch1 Properties window closes.

A port group named Unconfigured has been added.

Install ESXi software updates

To install available ESXi software updates, perform this procedure at the computer on which you installed the VMware Infrastructure Client:

1 Insert the *VMware ESXi 3.5 Update 3 Patch CD* into your computer's CD-ROM drive.

2 Select **Start > Programs > VMware > VMware Infrastructure Update**. The VMware Infrastructure Update window appears.

3 Load an update package from the patch CD:

  a In the Package Cache area, click **Add Files**. A pop-up window appears.

  b Browse to your CD-ROM drive and select the package zip file.

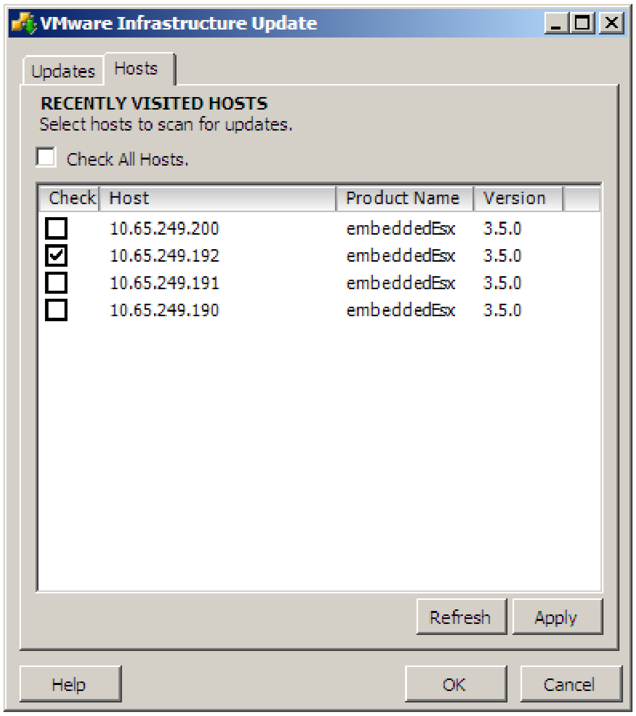
  c Click **Open**. The pop-up window closes and the package is added to the package cache. When the package is loaded, a pop-up window stating that the package does not contain applicable updates appears.

  d Click **OK**. The pop-up window closes.

4 [Conditional] If the *VMware ESXi 3.5 Update 3 Patch CD* contains multiple packages, repeat Step 3 for each additional package.

5 Click the **Hosts** tab.

Figure 21 Hosts tab



RECENTLY VISITED HOSTS
Select hosts to scan for updates.

□ Check All Hosts.

Check	Host	Product Name	Version
□	10.65.249.200	embeddedEsx	3.5.0
☑	10.65.249.192	embeddedEsx	3.5.0
□	10.65.249.191	embeddedEsx	3.5.0
□	10.65.249.190	embeddedEsx	3.5.0

6 In the list of recently visited hosts, select your 2150 VX appliance, and click **Apply**. A confirmation window appears.

7 Click **Yes**.

- If no updates are available, the No Updates Available window appears.

  Click **OK** to close the window. Continue to the next section, *Import multiple virtual appliances* on page 45.

- If updates are available, the Updates Available window appears. Continue with Step 8.

8 [Conditional] If updates are available, install them on your 2150 VX appliance:

- **a** Click **Install Updates**. An Update Progress window appears, and the Authenticate User for Install window appears.
- **b** Enter an administrative user and corresponding password for your 2150 VX appliance, and click **OK**. When the installation is complete, a message appears stating that your 2150 VX appliance has been updated.
- **c** Click **Continue**. The Update Progress window closes.
- **d** Using the VMware Infrastructure Client, connect to your 2150 VX appliance, click the **Summary** tab,, and click **Reboot**. The Confirm reboot window appears.
- **e** Click **Yes**. A Reboot window appears.
- **f** Enter an explanation for the restart, and click **OK**. Your 2150 VX appliance restarts.

Import multiple virtual appliances

To upload multiple virtual firewall and a virtual Control Center to your 2150 VX appliance:

- *Prepare your Windows-based computer* on page 45
- *Create a batch file to automate the import process* on page 46
- *Upload the virtual appliances* on page 46

To perform the procedures listed above, you will need the following items:

- McAfee Firewall Enterprisel 2150 VX appliance
- Windows-based computer with VMware Infrastructure Client installed
- VMware OVF Tool
- *McAfee Firewall Enterprise Virtual Appliance USB Drive*
- *McAfee Firewall Enterprise Control Center Virtual Appliance USB Drive*

Prepare your Windows-based computer

On your Windows-based computer:

1. Download the VMware OVF Tool at: *http://register.vmware.com/content/download-ovf-os.html*.
2. Extract the OVF Tool zip file.
3. On your C drive, create a new folder called **imaging**.
4. Move the contents of the extracted OVF Tool file to C:\imaging.
5. In the C:\imaging folder, run the **vcredist_x86** file to install the Microsoft Visual C Runtime.
6. Move the McAfee Firewall Enterprise virtual appliance file to the C:\imaging folder.
   - **a** Insert the *McAfee Firewall Enterprise Virtual Appliance USB Drive* into one of your computer's USB ports.
   - **b** Use Windows Explorer to view the contents of the USB drive, and extract the .zip file to C:\imaging.
   - **c** Remove the USB drive from your computer.
7. Move the Control Center file to the C:\imaging folder.
   - **a** Insert the *McAfee Firewall Enterprise Control Center Virtual Appliance USB Drive* into one of your computer's USB ports.
   - **b** Use Windows Explorer to view the contents of the USB drive, and extract the .zip file to C:\imaging.
   - **c** Remove the USB drive from your computer.

Create a batch file to automate the import process

1 Start Notepad: select **Start > Programs > Accessories > Notepad**.

2 In Notepad, type the five lines of text shown in Table 12. The line numbers are included for clarity only—do not type them.

Table 12 Batch file text

Line number	Text
1	`@echo off`
2	`REM This script should be called as follows:`
3	`REM uploadall <ESX server IP> <username> <password> <Firewall count>`

4	`ovftool "CommandCenter 4.0.0.03 2150VX.ovf"`
	`vi://%2:%3@%1?"net:Unconfigured=Unconfigured&"name="CommandCenter"`

5	`for /L %%X in (1,1,%4) do ovftool Secure_Firewall.ovf`
	`vi://%2:%3@%1?"net:Unconfigured=Unconfigured&"name="Secure Firewall`
	`%%X"`

3 Select **File > Save As**. The Save As window appears.

4 In the **File name** field, type `uploadall.bat`.

5 From the **Save as type** drop-down list, select **All Files**.

6 Click **Save**, and close Notepad.

Upload the virtual appliances

Run the batch file to upload the virtual appliances.

1 Open a command prompt and navigate to C:\imaging.

   a Select **Start > Programs > Accessories > Command Prompt**. The Command Prompt window appears.

   b Type `cd C:\imaging`, and press **Enter**.

2 Run the batch file.

   a Determine the number of virtual firewalls that you want to upload.

   b Type `uploadall` ***`ip username password count`***, where:

   - *ip* is the IP address of your 2150 VX appliance
   - *username* is an ESXi administrator name
   - *password* is that administrator's password
   - *count* is the number of virtual firewalls to upload

   c When you have finished typing the command, press **Enter**. A single Control Center and the specified number of virtual firewall uploads to your 2150 VX appliance.

Note: It takes about 45 minutes to upload 32 virtual firewalls over a gigabit network. If the OVF Tool shows the warning `There is no disk in the drive. Please insert a disk into drive D:`, right-click your CD-ROM drive in Windows Explorer, select Eject,, and close the drive.

McAfee
An Intel Company