McAfee®
An Intel Company

Installation Guide
Revision A

McAfee Firewall Enterprise 8.3.x

on CloudShield CS-4000 Platforms

COPYRIGHT

TRADEMARK ATTRIBUTIONS

Product and feature names and descriptions are subject to change without notice. Please visit mcafee.com for the most current products and features.

LICENSE INFORMATION

License Agreement

Contents

Preface

This guide provides the information you need to install your McAfee product.

Contents

About this guide

This information describes the guide's target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

Book title, *term*, *emphasis*	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input, code, message`	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext blue	A link to a topic or to an external website.
ℹ	**Note:** Additional information, like an alternate method of accessing an option.
💡	**Tip:** Suggestions and recommendations.
❗	**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning:** Critical advice to prevent bodily harm when using a hardware product.

Find product documentation

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task

1 Go to the McAfee Technical Support ServicePortal at http://mysupport.mcafee.com.

2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

CloudShield license information

Disclaimer

CloudShield Technologies, Inc. (CloudShield) assumes no responsibility for errors or omissions in this document. Nor does CloudShield make any commitment to update the information contained herein. Information in this document is provided in connection with CloudShield products only and is subject to change without notice.

No license, express or implied, to any intellectual property rights is granted by this document. The use of software is governed by the license agreement between the parties. Except as provided in CloudShield's Standard Terms and Conditions of sale, CloudShield assumes no liability whatsoever, and CloudShield disclaims any express or implied warranty relating to sale and/or use of CloudShield products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright, or other intellectual property right. CloudShield products are not intended for use in nuclear, medical, life saving, or life sustaining applications.

Note: Any unauthorized modifications to CloudShield products may void your warranty. Exceptions or requirements are contained in CloudShield's current warranty policy as provided at www.cloudshield.com.

Patents

6,661,119; 6,728,785; 6,737,763; 6,829,654; 7,082,502; 7,003,555; 7,114,008; 7,032,031; 7,210,022; 7,318,144; 7,330,908; 7,428,618; 7,437,482; 7,570,663; 7,624,142; 7,844,740;

Trademarks

CloudShield®, packetC®, CloudSentry®, and DNS Defender® are registered trademarks of CloudShield Technologies, Inc. in the United States.

BladeCenter® is a registered trademark of IBM. Eclipse is a trademark of the Eclipse Foundation.

1 Introduction

McAfee® Firewall Enterprise (Firewall Enterprise) is an application-based firewall that runs on CloudShield CS-4000 platforms to provide maximum security for high-assurance environments.

Contents

Firewall Enterprise overview

Firewall Enterprise allows you to protect your network from unauthorized users and attackers and to protect internal users as they access the Internet.

Firewall Enterprise features provide powerful configuration options that allow you to control user access to almost any publicly available service on the Internet while mitigating threats to your organization. Firewall Enterprise combines an application-layer firewall, user-based policy, IPsec VPN capabilities, SSL decryption, and McAfee® Global Threat Intelligence™ into one security appliance designed to offer centralized perimeter security.

Firewall Enterprise on CS-4000 platforms

The CS-4000 is a secure server platform that runs one or more instances of Firewall Enterprise.

Security features

The CS-4000 hardware and architecture provides increased security for the most hostile environments.

- All administrative communication to the CS-4000 is done remotely through an encrypted IPsec VPN tunnel.
- The CS-4000 does not contain any hard drives or permanent local storage. If a blade is removed or power is lost to a blade, no data is retained.
- The CS-4000 blades use anti-tamper technology that adheres to FIPS Level 3+ standards.

Unsupported features

When installed on CS-4000 platforms, some features are not supported on Firewall Enterprise.

- **High Availability** — High Availability is not supported, either between two firewall Content Processing Accelerators (CPAs) in the same chassis or across CS-4000 units.
- **Sendmail** — Because there is no permanent local storage on the CS-4000, any mail messages in the queue would be lost upon system restart.
- **Admin Console** — Management must be handled by McAfee® Firewall Enterprise Control Center (Control Center).
- **Link aggregation and interface redundancy** — NIC groups are not supported.
- **PPPoE** — PPPoE is not supported.
- **USB disaster recovery and USB installation** — There are no USB ports on the CS-4000.
- **VCD and alternate slice** — Due to the modified boot process of the CS-4000, the VCD and alternate slice are not accessible. The rollback capabilities of the virtual CPA (CPA-V) provide equivalent functionality.

Understanding CS-4000 architecture

Deployment of Firewall Enterprise on CS-4000 platforms requires two separate hardware components and specific network integration.

CS-4000 server

The CS-4000 is a 4U bladed, hardened chassis.

The CS-4000 features these hardware components:

- **Processing blades** — The CS-4000 houses up to three blades for packet processing. It supports any combination of two types of blades:
  - **Deep Packet Processing Module (DPPM)** — A DPPM uses programmable regex processing to inspect and handle network packets.
  - **Content Processing Accelerator (CPA)** — A single instance of Firewall Enterprise is installed on each CPA.

- **Chassis Management Module (CMM)** — The CMM establishes the IPsec VPN tunnel and controls administrative traffic to the server blades. Two CMMs can be installed, but only one is used in a Firewall Enterprise setup.
- **Interface Switch Module (ISM)** — The ISM provides network connectivity to the blades. It acts as a network patch panel between the external ethernet ports and the internal ports on the blades. Two ISMs, or one ISM and one ISM-XVR (crossover ISM), can be installed.

The chassis provides redundant fan units and power supplies. All components are fully hot-swappable.

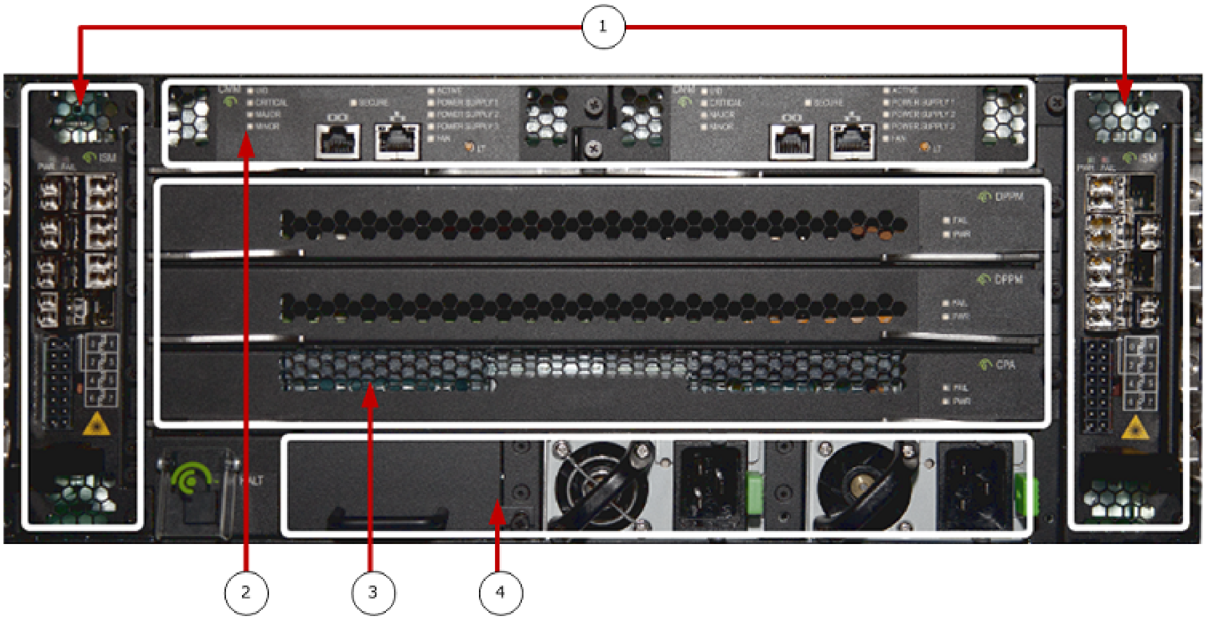

Figure 1-1 CS-4000 chassis front view

1	ISMs
2	CMMs
3	Processing blades
4	Power supplies

MC-CPOS server

The MC-CPOS (Multi-Chassis CloudShield Packet Operating System) server is a separate 1U server used for managing the CS-4000.

MC-CPOS, a Linux-based operating system designed and used by CloudShield, is the operating system used on the MC-CPOS server.

The MC-CPOS server hosts a CPA-V for each CPA blade. A CPA-V is a virtual machine that provides the PXE boot server used by a corresponding CPA blade.

Network integration

A minimum of two separate networks are needed for deployment — a secure management (*high-side*) network, and an unsecure (*low-side*) network.

When planning your network integration, consider these points:

- The MC-CPOS server must be placed in a physically secure location with access to the high-side network. Administrative access to the MC-CPOS server is restricted to the high-side network.
- The CS-4000 server is placed in the low-side network and is meant for unsecure physical environments. Communication between the CPA-V on the MC-CPOS and the CPA blade on the CS-4000 takes place through an IPsec VPN tunnel. This tunnel is not restricted to any network; depending on your environment, it might cross the low-side network, a separate network, or the Internet.
- The MC-CPOS server and the CPA-Vs have separate, unique IP addresses in the high-side network. You must also create an alias IP address on the MC-CPOS server for each CPA. This CPA alias address, which is also in the high-side network, is used by Control Center to manage the firewall on that CPA.

An MTU of 1500 is required for communication between the CS-4000 and MC-CPOS server.

The figure and table illustrate a general network integration using example IP addresses.

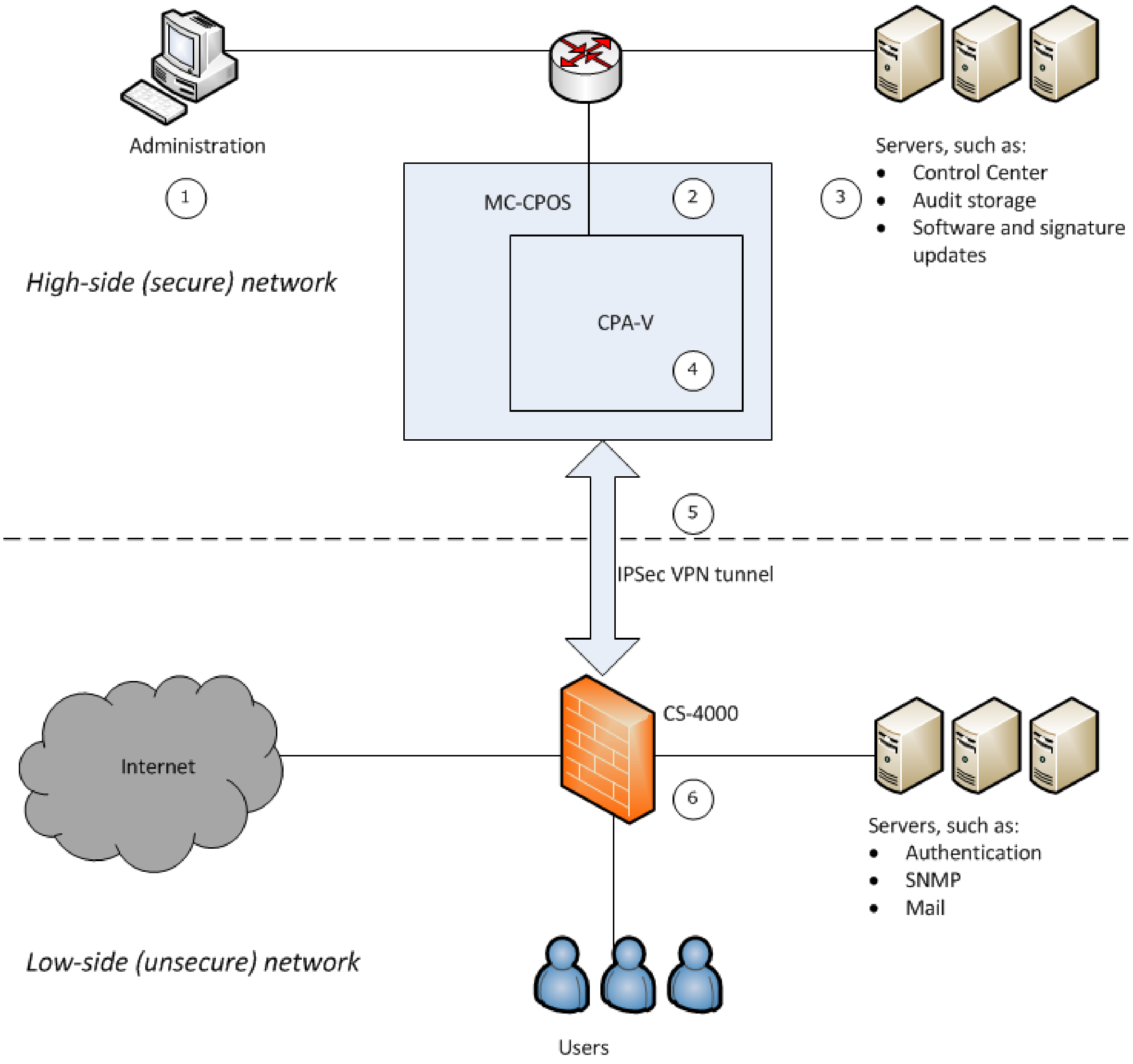

Figure 1-2 General CS-4000 network integration

Table 1-1 Example IP addresses

Reference	Component	IP or network address
MC-CPOS management network		10.1.1.0/24
1	MC-CPOS administration system	10.1.1.20
2	MC-CPOS management	10.1.1.100
CPA/CPA-V management network		10.1.2.0/24
3	Control Center Management Server	10.1.2.21
4	CPA-V 3 management	10.1.2.103
	CPA 3 management alias	10.1.2.133
Public VPN network		10.20.0.0/24
5	MC-CPOS VPN communication	10.20.0.1
	CS-4000 CMM VPN communication	10.20.0.2

Table 1-1 Example IP addresses *(continued)*

Reference	Component	IP or network address
Private VPN network ℹ The private VPN IP addresses are static and cannot be changed.		169.254.0.0/16
5	CPA-V 3 VPN communication	169.254.11.13
	CPA 3 VPN communication	169.254.1.13
Firewall Enterprise (CPA 3) external network		192.168.0.0/24
6	Firewall Enterprise (CPA 3) external interface	192.168.0.1
Firewall Enterprise (CPA 3) internal network		192.168.1.0/24
6	Firewall Enterprise (CPA 3) internal interface	192.168.1.1

2 Planning deployment

Prepare your environment for integrating Firewall Enterprise on a CloudShield CS-4000 platform.

Contents

Documentation requirements

Additional documentation is required to manage Firewall Enterprise on CS-4000 platforms.

Table 2-1 Required documents

Source	Documents
McAfee	• Grant letter containing download, activation, and support information • *McAfee Firewall Enterprise Release Notes* • *McAfee Firewall Enterprise Product Guide* • *McAfee Firewall Enterprise Control Center Quick Start Guide* • *McAfee Firewall Enterprise Control Center Product Guide*
CloudShield	• *CS-4000 Installation Guide* • *CS-4000 System Administration Guide*

Firewall Enterprise management requirements

A Control Center Management Server is required to manage Firewall Enterprise on CS-4000 platforms.

- The Management Server must be at version 5.3.0 or later.
- The Management Server must be connected to the secure network of the MC-CPOS server.
- A Microsoft Windows-based computer is needed to host the Control Center Client application.

MC-CPOS and CS-4000 configuration prerequisites

Before you can install and configure Firewall Enterprise, you must install and perform basic configuration on the MC-CPOS and CS-4000 servers.

This includes:

- Racking the MC-CPOS and CS-4000 servers
- Turning on all CS-4000 server blades
- Installing the MC-CPOS server software
- Performing network and IP address configuration on the MC-CPOS and CS-4000 servers, including addresses for management, VPN communication, and the CPA-Vs
- Configuring the ISM port mappings
- Establishing the VPN tunnel

To set up the MC-CPOS and CS-4000 servers, follow the instructions in the *CS-4000 Installation Guide*. To make sure your setup is successful, log on to each default CPA-V and ping the corresponding CPA.

> Do not use the installation guide to install applications on the CPA.

3 Installing Firewall Enterprise

Installing Firewall Enterprise requires installing the CPA-V, performing initial configuration, and restarting the CPA blade.

Contents

Download and install the CPA-V

The CPA-V template contains the PXE server used to install Firewall Enterprise on the CPA.

Tasks

- *Download the CPA-V template* on page 17
  Download the CPA-V template from the McAfee downloads page to an SSH server reachable by the MC-CPOS server.
- *Load and install the template* on page 18
  On the MC-CPOS server, load and install the CPA-V template.

Download the CPA-V template

Download the CPA-V template from the McAfee downloads page to an SSH server reachable by the MC-CPOS server.

> **Before you begin**
>
> Locate your grant number.

Task

1. In a web browser, go to www.mcafee.com/us/downloads.
2. Enter your grant number, then select the appropriate product and version.
3. Download the CPA-V template file.
4. Extract the .qcow template file from the .gz file.

Load and install the template

On the MC-CPOS server, load and install the CPA-V template.

Task

1 Using a command line session, log on to the MC-CPOS server and use SCP to upload the template from the SSH server.

  a Enter:

```
file-mgr upload file-name filename ip-address ipaddr method scp login username
```

  where *filename* is the full path and name of the template file, *ipaddr* is the IP address of the SSH server, and *username* is the user.

  b When prompted, enter the password for the SSH server. A message appears indicating the file is uploading.

  c Check if the upload has completed. Enter:

```
show file-mgr upload-status
```

  The list of templates and status appears.

2 Import the template file.

  a Enter:

```
vm import-template template-name filename
```

  where *filename* is the name of the template file.

  b Verify the template was imported. Enter:

```
show vm display-templates
```

  A list of imported templates appears.

3 Install the CPA-V template.

  a Enter `config` to change to configuration mode. The config prompt appears.

  b Enter:

```
cpa slot number vm template-name filename start-method reuse-instance
```

  where *number* is the number of the corresponding blade and *filename* is the name of the template file.

  c Commit the changes by entering `commit`.

  d Exit configuration mode. Enter `exit`, then enter `exit` again. The operational mode prompt appears.

4 Restart the CPA-V.

  a Enter:

```
chassis slot blade-number vm-restart
```

  where *blade-number* is the word, *blade*, followed by the number of the blade.

  Example: `chassis slot blade3 vm-restart`

b. When prompted to restart, enter `yes`. The CPA-V restarts.

> The CPA-V might take ten minutes or more to restart.

c. Check the status of the CPA-V. Enter:

```
show vm domain-info domain-state
```

If the CPA-V finished restarting, the status of that slot is *running*.

Perform the initial configuration

Use the mfeconfig utility to enter the initial configuration. You can also enable the network console and netdump features.

Task

1. From the administrative system, use a command line session to log on to the CPA-V.

   > The default user name for the CPA-V is `root` and the default password is `cloudshield`. McAfee strongly recommends changing this password by using the `passwd` command.

2. Enter the command:

   ```
   mfeconfig
   ```

   The mfeconfig utility appears.

3. If this is your first time running the mfeconfig utility, accept the license agreement.

4. Type **1** to select the initial configuration.

   > You can also use the up and down keys, followed by **Enter**, to select an option.

5. From the **Basic settings** menu, select an option and type the information as appropriate. When finished, press **Enter** to save the changes or **Esc** to discard the changes. Each of the six options must be configured:

   - **1 — Set alias address and netmask in CIDR format**

     This is the alias on the CPA-V used for managing Firewall Enterprise. The alias must belong to the high-side network.

   - **2 — Set hosts/networks to route through the CPA-V**

     This list includes any device needed to manage Firewall Enterprise, such as the Control Center Management Server.

     > When entering networks, use the up and down arrows to add new lines. When finished, press **Enter**.

- **3 — Set firewall administrator's username**
- **4 — Set firewall administrator's password**

  The firewall user name and password are different from the users you specify as part of the Control Center installation and initial configuration.

- **5 — Set firewall's hostname**
- **6 — Set firewall's DNS resolver**

6 Type **8** to save your changes.

7 Select the 8.3.x package for a new installation.

  a At the **Welcome to mfeconfig!** menu, type **3** to enter installation options.

  a At the **Install options** menu, type **2**.

  b In the **Edit fresh install package** list, press **Enter** to select a package and return to the previous menu.

  c Type **5** to save your changes.

8 At the **Welcome to mfeconfig!** menu, type **4** to exit mfeconfig.

  If you want to enable the network console or netdump, do not exit mfeconfig at this time. Perform the tasks in the next sections.

After performing the initial configuration and exiting mfeconfig for the first time, the CPA automatically restarts.

Depending on the connection speed between the MC-CPOS server and the CS-4000, the restart and installation might take 15–25 minutes or more.

See also

Network integration on page 12

Enable the network console

The CS-4000 does not have a serial port or VGA port. You can configure the firewall to send console output over the network to the CPA-V. This configuration is recommended but optional.

McAfee highly recommends enabling the network console during initial configuration. If you choose to enable the network console at a later time, you must restart the CPA for the change to take effect.

Task

1 Using a command line session, log on to the CPA-V and enter:

```
mfeconfig
```

  The mfeconfig utility appears.

2 Type **2** to select debugging options.

  You can also use the up and down keys to select an option, followed by **Enter**.

3 In the **Debug options** menu, type **1**.

4 In the **Edit network console** menu, use the up arrow to move the cursor position to **On**, then press **Enter**.

5 In the **Debug options** menu, type **4** to save your changes.

6 At the **Welcome to mfeconfig!** menu, type **4** to exit mfeconfig.

See also
Connect to the firewall CPA with the network console on page 25

Enable netdump

You can configure the firewall to send core dump files to the MC-CPOS server in the event of a kernel crash. This configuration is recommended but optional.

When a system encounters a kernel crash, it writes a core file to the local disk used for debugging purposes. In some cases, a restart is required to recover from a kernel crash. Because the CS-4000 does not have any permanent local storage, the core file will be removed at restart. In order to preserve core files generated from a kernel crash, you must enable the netdump option.

Netdump uses UDP ports 20023 and 20024.

> McAfee highly recommends enabling netdump during initial configuration. If you choose to enable netdump at a later time, you must restart the CPA for the change to take effect.

Task

1 Using a command line session, log on to the CPA-V and enter:

```
mfeconfig
```

The mfeconfig utility appears.

2 Type **2** to select debugging options.

> You can also use the up and down keys to select an option, followed by **Enter**.

3 In the **Debug options** menu, type **2**.

4 In the **Edit netdump** menu, use the up arrow to move the cursor position to **On**, then press **Enter**.

5 In the **Debug options** menu, type **4** to save your changes.

6 At the **Welcome to mfeconfig!** menu, type **4** to exit mfeconfig.

Core dump files resulting from a kernel crash are stored in /var/chroot/home/mfe/cores.

4 Post-installation tasks

Register the firewall to Control Center and complete additional firewall configurations.

Contents

Register the firewall to Control Center

Use the Control Center Client application to register the firewall to the Control Center Management Server.

Task

1. From the Control Center Client application, select **Policy**.
2. From the **Policy** tree, right-click the **Firewalls** node and select **Add Object**. The **Add New Firewall Wizard** appears.
3. On the **Firewall Connection Information** page, enter the information.

   ⓘ The firewall IP address is the same CPA alias address you entered in *Perform the initial configuration*.

4. Click **Next**. The **Firewall Registration Information** page appears.
5. Select **Register the firewall with this Management Server.**
6. In the **SSH username** and **password** fields, enter the Firewall Enterprise administrator username and password.
7. Click **Next**. The **Summary** page appears.
8. Click **Register**. The **Registration Status** page appears.
9. When the firewall registration completes, click **Next**. The **Retrieval of the Firewall into Control Center** page appears.
10. Click **Finish** to complete the wizard and add the firewall to Control Center.

Perform post-setup configurations

Several post-setup tasks are needed for Firewall Enterprise. These are high-level steps; for detailed instructions, refer to the *McAfee Firewall Enterprise Control Center Product Guide*.

Task

1. Configure the license.
2. Configure zones and interfaces.
3. Configure the default route.
4. Configure rules and policy.
5. Configure audit archiving.

> Because the CS-4000 does not have any permanent local storage, McAfee strongly recommends exporting firewall audit to another network device, such a syslog server, an FTP or SCP server, or the Control Center Management Server.

5 Maintenance and troubleshooting

If you experience system problems with your firewall, use the network console for troubleshooting, or re-install the firewall.

Contents

Connect to the firewall CPA with the network console

In the event that Firewall Enterprise is unresponsive, use the network console for troubleshooting.

The network console communication uses UDP port 54321.

Task

1 Using a command line session, log on to the CPA-V and enter:

```
dconsclient ipaddr
```

where *ipaddr* is the IP address of the CPA blade. Depending on the CPA, use one of these IP addresses:

- CPA 1 — 169.254.1.11
- CPA 2 — 169.254.1.12
- CPA 3 — 169.254.1.13

The firewall console appears.

2 Type this sequence to disconnect from the console:

```
Enter
~ (tilda)
. (period)
```

See also

Enable the network console on page 20

Re-install the firewall

Due to the nature of the CS-4000 hardware, a re-installation and re-application of policy is done every time Firewall Enterprise restarts. However, there may be other cases where you want to re-install the firewall to the minimum configuration.

Task

1 Using a command line session, log on to the CPA-V and enter:

```
mfeconfig
```

The mfeconfig utility appears.

2 Type **3** to select install options.

> You can also use the up and down keys, followed by **Enter**, to select an option.

3 At the **Install options** menu, type **2**.

4 In the **Edit fresh install package** list, press **Enter** to select a package and return to the previous menu.

> Use the space key to select multiple packages.

5 Type **5** to save your changes.

6 At the **Welcome to mfeconfig!** menu, type **4** to exit mfeconfig.

The firewall will re-install to the minimum configuration after the next CPA restart.

Restart the CPA

Restarting the CPA will reinstall the firewall, apply mfeconfig settings, apply patches, and restore a configuration backup.

Task

1 Using a command line session, log on to the MC-CPOS server. Enter this command to restart the CPA blade:

```
blade number reboot
```

Where *number* is the number of the blade.

Example: `blade 3 reboot`

2 When prompted, enter `yes`.

The blade restarts and installs Firewall Enterprise.

> Depending on the connection speed between the MC-CPOS server and the CS-4000, the restart and installation might take 15–25 minutes or more.

Restoring lost VPN keys

In certain situations, the CS-4000 will remove its hard-coded IPsec VPN keys as a security measure.

The CS-4000 will lose the VPN keys under these conditions:

- Forcibly opening any of the CS-4000 blades
- Subjecting the unit to extreme hot or cold temperatures

If the VPN keys are lost, the CS-4000 unit must be returned to the manufacturer for restoration. Call McAfee technical support for assistance.

Index