Common Criteria Evaluated Configuration Guide

Revision A

McAfee Firewall Enterprise 8.3.2

The *McAfee Firewall Enterprise Common Criteria Configuration Guide*, version 8.3.2, describes requirements and guidelines for installing, configuring, and maintaining a McAfee® Firewall Enterprise (Firewall Enterprise) appliance to comply with Common Criteria evaluation standards.

About this guide

This document states the parameters and requirements for setting up and maintaining a Firewall Enterprise to run in a Common Criteria-evaluated configuration. If your organization's security policy requires the Firewall Enterprise appliance to match the Common Criteria Target of Evaluation (TOE) configuration, carefully follow the instructions in this document.

- Understanding Common Criteria
- Establishing the TOE environment
- Preparing for a TOE installation
- Install and configure an unmanaged firewall
- Set up a TOE configuration for Control Center
- Install and configure a managed firewall
- Maintain a TOE configuration

Download additional McAfee documentation

This guide is the primary document for configuring Firewall Enterprise in a TOE environment. In addition to this guide, see the following documentation to plan and implement a TOE configuration.

These documents provide information about general networking concepts and all firewall services, features, and navigation.

These documents can be followed only when they meet TOE requirements. All configurations specified in this document take precedence over other McAfee documentation.

Task

1 Go to the McAfee ServicePortal at http://support.mcafee.com and click **Knowledge Center**.

2 Enter a product name, select a version, then click **Search** to display a list of documents.

3 Select the documentation relevant to your environment:

- *McAfee Firewall Enterprise Product Guide*, version 8.3.2
- *McAfee Firewall Enterprise, Virtual Appliance Installation Guide*, version 8.x
- *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x
- *McAfee Firewall Enterprise Release Notes*, version 8.3.2
- *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2
- *McAfee Firewall Enterprise Control Center Installation and Migration Guide*, version 5.3.2
- *McAfee Firewall Enterprise Control Center Release Notes*, version 5.3.2
- *McAfee Firewall Enterprise Control Center FIPS 140-2 Configuration Guide*

Download the McAfee Firewall Enterprise Security Target

The *McAfee Firewall Enterprise Security Target* is a document provided by Common Criteria that identifies security requirements for Firewall Enterprise. The document can be found on the international Common Criteria webpage.

Task

1 Visit www.commoncriteriaportal.org/products/.

2 Select **Boundary Protection Devices and Systems**.

3 Search for **McAfee Firewall Enterprise v8.3.2**.

4 Click the **Security Target** link.

About Common Criteria

Common Criteria represents the outcome of a series of efforts to develop criteria for evaluation of information technology (IT) security products. The criteria and evaluation standards are broadly used and respected within the international community.

Many organizations require that their security products be Common Criteria certified. The McAfee Firewall Enterprise software version 8.3.2 has been submitted for Common Criteria certification at Evaluation Assurance Level 4 Augmented (EAL 4+) with compliance to the Department of Defense (DoD) Application Firewall Protection Profile for Basic Robustness Environments.

In this document, Firewall Enterprise refers to McAfee Firewall Enterprise in the evaluated configuration as the Target of Evaluation (TOE). This document explains how to install and use the *TOE* configuration. This document applies to Firewall Enterprise version 8.3.2 and McAfee® Firewall Enterprise Control Center (Control Center) version 5.3.2.

References to the TOE configuration imply that Firewall Enterprise is installed and configured as described in the *McAfee Firewall Enterprise Security Target* document.

For more information about Common Criteria, McAfee, Inc., and McAfee® Firewall Enterprise evaluation level requirements, visit www.commoncriteriaportal.org.

Establishing the TOE environment

Prepare for integrating Firewall Enterprise into your network.

Before installing Firewall Enterprise, your environment must follow TOE requirements.

The *McAfee Firewall Enterprise Product Guide*, version 8.3.2 (product guide) can be used as a supplement to this document, but it can only be used when it meets the TOE requirements.

TOE environment assumptions

The TOE assures effective security measures in a cooperative, non-hostile environment when correctly installed and managed. Make sure the TOE environment meets the necessary assumptions and security requirements.

The environment for the TOE should be managed to satisfy the following assumptions:

- The TOE is physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities is considered low.
- The TOE appliance, or the virtual machine in which TOE is hosted, does not host public data.
- Authorized administrators are non-hostile and follow all administrator guidance; however, they are capable of error.
- The TOE must be delivered, installed, administered, and operated in a manner that maintains security.
- There are no general purpose computing capabilities (for example, the ability to execute arbitrary code or applications) or storage repository capabilities on the TOE, on the authentication server, or on the local administration platform.
- Authorized administrators can access the TOE remotely from the internal and external networks.

Because the authentication server and the local administration platform play a critical role in the TOE enforcement of the security policy, the following conditions are assumed to exist with respect to the authentication server and the local administration platform:

- The authentication server and local administration platform are physically secure.
- The threat of malicious attacks aimed at discovering exploitable vulnerabilities in the authentication server and local administration platform is considered low.
- The communication path between the TOE (authentication client) and the single-use authentication server is physically protected.
- The authentication server and local administration platform do not host public data.
- Authorized administrators of the authentication server and local administration platform are non-hostile and follow all administrator guidance; however, they are capable of error.

TOE security environment considerations

The TOE environment must be established and managed to meet these physical and logical constraints.

- The configured TOE shall manage traffic for at least two (2) networks, with at least one being designated as internal and one being designated as external.
- The administrators can manage the TOE locally and remotely.
- The configured TOE shall be managed from an administrative workstation running on a Windows operating system.

- The environment shall include a single-use authentication mechanism that is compatible with TOE, such as any RADIUS server.
- The single-use authentication device itself shall prevent the reuse of authentication data related to human users (also remote administrator connections) sending or receiving FTP or Telnet information.
- Physical access to the administrative workstation and single-use authentication devices shall be controlled along with the TOE and the network link connecting them.

Preparing for a TOE installation

Follow these guidelines using the *Planning* chapter of the product guide to set up Firewall Enterprise in a manner that meets the TOE configuration.

These guidelines and requirements are most often exceptions to the instructions written in the product guide.

- If a feature or service is listed, configure the mentioned item as described in this section.
- If a feature or service is not listed, configure it as written in the product guide.

Check your shipment

Verify that you received a secure delivery of the correct appliance model.

Task

1. Examine the outside packaging and markings of the delivery carton containing the appliance to ensure that it arrived via an approved commercial carrier from McAfee, Inc.
2. Examine the shipping and tracking information available with the package to look for any unexpected information related to the timing and route for the shipment. If there is any doubt about the veracity of the shipment, contact McAfee, Inc., Customer Service to confirm that the product was indeed ordered by your organization and sent by McAfee, Inc.
3. Verify that the shipping carton has McAfee, Inc., and McAfee logos as depicted on the McAfee, Inc., website. Ensure the package openings are securely sealed with tamper-evident materials that have not been damaged. Also, check the carton to make sure there is no evidence that seals have been removed, as that would cause damage to the surfaces of the container.
4. Examine the interior contents of the package containing the appliance to ensure that it also contains printed materials with McAfee, Inc., markings similar to those depicted on the McAfee, Inc., website.

Create your password

These guidelines for creating and managing Firewall Enterprise administrator and user passwords supplement the password guidance included in the product guide.

Strong passwords are a vital part of ensuring network security. Make sure that all passwords are created and changed in a manner that meets these following requirements when using the graphical user interface.

Task

1 Create your password. Make sure that all passwords are created and changed in a manner that meets the following requirements when using the graphical user interface:

- Make the minimum password length at least 12 characters, not to exceed 64 maximum characters.
- Include mixed-case alphabetic characters.
- Include at least one non-alphabetic character.
- The Firewall Enterprise operated in a Common Criteria-evaluated configuration supports passwords created from letters, numbers, and special characters. The following set of 94 characters can be used in a password:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

1234567890

!"#$%&'()*+,-./:;<@[\`{|=>?]^_}~
```

A keyboard that provides the 94 characters is required for the TOE (for example, a U.S. keyboard).

2 Record your password for use during installation and configuration.

Complete additional pre-installation tasks

Check these items before proceeding with the Firewall Enterprise installation.

Task

1 While creating your installation plan, incorporate the following special requirements:

- Use two network interfaces for managed traffic: one for an internal zone and one for an external zone.
- Consider using a third network interface for an administrative zone. This network interface will connect Firewall Enterprise to the administrator workstation and to the authentication server.
- Use a transparent DNS configuration.
- Use the **Allow administrative services only** feature instead of enabling the **Allow administrative and basic outbound Internet services** feature. This prohibits non-administrative traffic.
- Use remote administration on the internal zone to begin with.
- Activate a BIOS password on the appliance.

2 For VMware deployments:

- Make sure the latest security patches have been applied to the ESXi server.
- Harden the VMware implementation using the latest VMware vSphere Security Hardening Guide, and implement steps appropriate for the particular operational environment.
- Make sure the ESXi management network (VMkernel port) is configured to reside on the same administrative zone network as the Admin Console.

Install and configure an unmanaged firewall

Follow these guidelines when using the product guide to install and configure Firewall Enterprise in a manner that meets the TOE configuration.

Consider the following:

- These guidelines and requirements are most often exceptions to the instructions written in the product guide.
- For each task listed below, configure the mentioned item as described in this section. If a feature or service is not listed below, configure it as written in the product guide.

> The instructions in this section only apply to firewalls that are not managed by Control Center. If your firewall is managed by Control Center (including firewalls on Crossbeam X-Series platforms), follow the instructions in the *Set up a TOE configuration for Control Center* and *Install and configure a managed firewall* sections.

Tasks

- *Install the management tools and create the initial configuration on an unmanaged firewall* on page 6
  Follow the instructions in the *Setup* chapter of the product guide to set up the Admin Console administration software on a Windows-based computer.
- *Install Firewall Enterprise software on an unmanaged firewall* on page 7
  You must bring the software to a version that meets the TOE guidelines.
- *Complete the initial setup on an unmanaged firewall* on page 7
  Complete the initial setup, seeing the product guide as needed.
- *Configure password requirements on an unmanaged firewall* on page 8
  Configure the password requirements as described in *Create your password*.

Install the management tools and create the initial configuration on an unmanaged firewall

Follow the instructions in the *Setup* chapter of the product guide to set up the Admin Console administration software on a Windows-based computer.

> The Admin Console must be installed on a computer in the firewall internal zone.

The following special requirements must be followed when setting up the hardware and running the Quick Start wizard:

Task

1 Select **Create Configuration**.

2 Select **Allow administrative services only**.

> Do not enter a remote administration route.

3 [Conditional] If you select the **Save Configuration** option, maintain the security of the saved configuration.

> The saved configuration contains password information that must be safeguarded. To prevent tampering when not in use, store the saved configuration on a USB drive or other storage media in a secure, controlled location. This security ensures the integrity of the initial configuration.

See also

Set up a TOE configuration for Control Center on page 8

Install Firewall Enterprise software on an unmanaged firewall

You must bring the software to a version that meets the TOE guidelines.

Task

1. Plan for a new installation, even if the software is preloaded.
2. [Hardware appliances only] Use a local console (keyboard and monitor, or serial terminal) to install the software on Firewall Enterprise.
3. Install version 8.3.2 software. Follow the instructions in the *McAfee Firewall Enterprise Release Notes*, version 8.3.2, *Perform a new installation*.

Complete the initial setup on an unmanaged firewall

Complete the initial setup, seeing the product guide as needed.

Task

1. License the firewall. For instructions, see the product guide, *License a firewall on an isolated network*.
2. Configure the zone settings.
3. Make these Admin Console File Editor changes:
   a. Use the Admin Console File Editor and open the /etc/rc.local file.
   b. Add the following line to the /etc/rc.local file for each of the locally attached routers/gateways:

      ```
      arp -s IP_ADDR MAC_ADDR
      ```

      where:

      IP_ADDR = the IP address of the router/gateway

      MAC_ADDR = the MAC address of the router/gateway in the following format:

      xx:xx:xx:xx:xx:xx

      This change creates a static ARP entry for the local routers/gateways.

      If the MAC address for any of these IP addresses changes, the respective entries must be updated.

   c. Add the following line to the /etc/rc.local file:

      ```
      cf audit mod filter name="TCP SYN Attack" sacap_filter="event
      AUDIT_R_NET_TCP_SYNATTACK && ! src_ip IP_ADDR/32" number=11 filter_type=attack
      ```

      where *IP_ADDR* is the IP address of the default gateway for Firewall Enterprise. This change prevents your default gateway's IP address from triggering a TCP SYN Attack filter.

   d. Use the Admin Console file editor to open the /etc/ttys file and find this line:

      ```
      console none unknown off secure
      ```

      Change `secure` to `insecure` if not already set as such. This change ensures that administration authentication is required if there is a failure during the boot sequence or when the system starts up to emergency maintenance mode.

4 Use the Admin Console to set the IP network defense as follows:

   a Select **Policy** | **Network Defenses** and click the **IP** tab.

   b [Conditional] If not already enabled, select **source broadcast address** and **incorrect source address for interface**.

   c Click **Save**.

   d Confirm the selection of **incorrect source address for interface**.

5 Make sure that the authentication failure lockout options are configured with the necessary integer limit on the external authentication servers. Use the Admin Console to configure one or more external authentication servers. See the *Identity validation* chapter of the product guide for instructions.

6 Create a configuration backup. See the *General maintenance* chapter of the product guide, *Backing up and restoring the firewall configuration*, for instructions.

7 Use the information in the *Complete post-startup tasks* section of the product guide for reference only. All these additional tasks can only be done if they comply with the instructions in this document. Do not configure Firewall Enterprise for SSH or Telnet administration. The command line interface cannot be used to maintain a TOE configuration.

Configure password requirements on an unmanaged firewall

Configure the password requirements as described in *Create your password*.

Task

For option definitions, press **F1** or click **Help** in the interface.

1 Select **Policy** | **Rule Elements** | **Authenticators** | **Password**.

2 Click the **General** tab.

3 In the **Password Requirements** area, **Minimum Password Length** field, enter `12`.

4 Select the **Require complex passwords** option and enter the following values:

   - In the **Require** *n* **of the four character groups in every password** field, enter `3`.
   - In the **Require at least** *n* **character(s) per required group in every password** field, enter `1`.

   There might be a delay in the password expiration. Do not rely on this setting.

5 If using external authentication, authentication failure lockout handling must be set on external authentication servers such as RADIUS, LDAP, and Microsoft Windows Domain.

Set up a TOE configuration for Control Center

Set up McAfee Firewall Enterprise Control Center to meet the TOE configuration.

Control Center is optional for managing some firewalls.

- **Optional**
  - Hardware appliances
  - Virtual appliances
- **Mandatory** — Crossbeam X-Series Platforms

Follow these guidelines when using the *McAfee Firewall Enterprise Control Center Product Guide*, version 5.3.2 (Control Center product guide), to install and configure Control Center in a manner that meets the TOE configuration.

Using Control Center to manage firewalls is not mandatory for a TOE environment.

Tasks

- *Install Control Center software* on page 9
  Install the Control Center to the correct version and patch level.
- *Enable Control Center for FIPS 140-2 processing* on page 10
  With FIPS 140-2 processing enabled, the system uses FIPS 140-2-approved cryptographic libraries and key lengths, and runs FIPS 140-2 self-tests.
- *Set up the audit trail archive* on page 10
  Enable audit tracking on the Control Center Management Server.
- *Configure hard disk settings* on page 10
  To prevent audit data loss, configure the Control Center to shut down cryptographic operations if the logs or database partitions of the Management Server are full.
- *Configure account lockout settings* on page 11
  If you are using local Control Center passwords, configure Control Center to permanently lock out accounts when multiple failed logon attempts occur.

Install Control Center software

Install the Control Center to the correct version and patch level.

You must perform a new installation on the Control Center. It cannot be upgraded from a previous installation.

Task

1. Install version 5.3.2 of the Control Center Client application. Follow the instructions in the *McAfee Firewall Enterprise Control Center Installation and Migration Guide*.
2. Install version 5.3.2 of the Control Center Management Server.
   - **Hardware appliances** — Follow the instructions in the *McAfee Firewall Enterprise Control Center Installation and Migration Guide*.
   - **Virtual appliances** — Follow the instructions in the *McAfee Firewall Enterprise Control Center Installation and Migration Guide*, version 5.3.2 to install a new VMware image.
   - **5.2.x users** — Follow these steps:
     1. Migrate to version 5.3.0.
     2. Upgrade to version 5.3.1.
     3. Upgrade to version 5.3.2.
     4. Enable FIPS as detailed in this guide.
3. Configure the appliance manually. Do not use the Control Center Initialization Tool to configure the Control Center.

Do not configure the Remote Management Module (RMM3) on a FIPS 140-2-compliant Control Center.

Enable Control Center for FIPS 140-2 processing

With FIPS 140-2 processing enabled, the system uses FIPS 140-2-approved cryptographic libraries and key lengths, and runs FIPS 140-2 self-tests.

FIPS 140-2 processing is required for Common Criteria compliance, even for Control Center appliances that are not FIPS 140-2-compliant.

Task

For option definitions, press **F1** or click **Help** in the interface.

1. Start the Control Center Client application and log on to the Control Center Management Server.
2. Select **Control Center** | **Settings** | **FIPS**. The **FIPS** window appears.
3. Select **Require FIPS 140-2 processing**, then click **OK**. A message appears.
4. Click **OK**.

The Control Center restarts with FIPS 140-2 processing enabled. When you log on to the Control Center Management Server again, **FIPS 140-2 processing enabled** appears on the Client application title bar.

For more information on running Control Center in the FIPS 140-2 validated mode, see the *McAfee Firewall Enterprise Control Center FIPS 140-2 Configuration Guide*.

Set up the audit trail archive

Enable audit tracking on the Control Center Management Server.

Task

For option definitions, press **F1** or click **Help** in the interface.

1. From the Control Center Client application, select **Control Center** | **Audit Trail** | **Settings** | **Archive Settings**. The **Archive Settings** tab appears.
2. Select **Archive audit data**.
3. Configure archive settings as needed, then click **OK**.

Control Center audit is stored in the Control Center Management Server database until it is archived to another location or removed.

When examining crypto logs from Control Center, SSH entries do not include the year. Using a custom time range will prevent any SSH entries from being displayed.

Configure hard disk settings

To prevent audit data loss, configure the Control Center to shut down cryptographic operations if the logs or database partitions of the Management Server are full.

Shutting down cryptographic operations prevents remote access to the Control Center Management Server using SSH or from the Control Center Client application.

Task

For option definitions, press **F1** or click **Help** in the interface.

1 From the Control Center Client application, select **Control Center** | **Settings** | **Hard Disk**. The **Hard Disk Settings** window appears.

2 Select **Prevent loss of audit data**.

3 Click **OK**.

All cryptographic operations will be shut down if either the logs or the database partition on the Management Server is full.

Configure account lockout settings

If you are using local Control Center passwords, configure Control Center to permanently lock out accounts when multiple failed logon attempts occur.

Task

For option definitions, press **F1** or click **Help** in the interface.

1 From the Control Center Client application, select **Control Center** | **Settings** | **System**. The **System Settings** window appears.

2 On the **Client Settings** tab, select **Account lockout is permanent**.

Accounts that are locked out remain locked out until reset by an administrator.

If one-time passwords are used for authentication on Control Center, make sure that the authentication lockout options are configured as needed on the external authentication servers. For more information on configuring Control Center for external authentication, see the *Control Center settings* chapter of the Control Center product guide for instructions.

Install and configure a managed firewall

Follow these guidelines when using the Control Center product guide to install and configure Firewall Enterprise in a manner that meets the TOE configuration.

Consider the following:

- These guidelines and requirements are most often exceptions to the instructions written in the Control Center product guide.
- For each task listed here, you must configure the mentioned item as described in this section. If a feature or service is not listed, configure it as written in the Control Center product guide.

The instructions in this section only apply to firewalls that are managed by Control Center. If you are not using Control Center to manage your firewall, follow the instructions in *Install and configure an unmanaged firewall*.

Tasks

- *Create the initial configuration on a managed firewall* on page 12
  Follow these special requirements when setting up the firewall and running the Quick Start Wizard.
- *Install Firewall Enterprise software on a managed firewall* on page 12
  You must bring the software to the version that meets the TOE guidelines.
- *Add a managed Firewall Enterprise to Control Center* on page 13
  If you are using Control Center to maintain the TOE configuration, register the firewall with the Control Center. The method you use depends on whether you are using hardware and virtual appliances, or Crossbeam X-Series Platform.
- *Complete the initial setup on a managed firewall* on page 15
  Complete the initial setup, seeing the Control Center product guide as needed.
- *Configure password requirements on a managed firewall* on page 16
  Configure the password requirements as described in *Create your password*.

See also

Install and configure an unmanaged firewall on page 6

Create the initial configuration on a managed firewall

Follow these special requirements when setting up the firewall and running the Quick Start Wizard.

Task

1 Select **Create Configuration**.

2 Select **Allow administrative services only**.

3 Do not enter a remote administration route.

4 If you select the **Save Configuration** option, you must maintain the security of the saved configuration.

The saved configuration contains password information that must be safeguarded. To prevent tampering when not in use, store the saved configuration on a USB drive or other storage media in a secure, controlled location. This ensures the integrity of the initial configuration.

Install Firewall Enterprise software on a managed firewall

You must bring the software to the version that meets the TOE guidelines.

Task

1 Plan for a new installation, even if the software is preloaded.

2 [Hardware appliances only] Use a local console (keyboard and monitor, or serial terminal) to install the software on Firewall Enterprise.

3 Bring the firewall to version 8.3.2.

- **Hardware appliances and virtual appliances** — Install version 8.3.2 software. Follow the instructions in the *McAfee Firewall Enterprise Release Notes*, version 8.3.2, *Perform a new installation*.
- **Crossbeam X-Series** — Install version 8.3.2 software. Follow the instructions in the *McAfee Firewall Enterprise Release Notes*, version 8.3.2, *Perform a new installation*.

Add a managed Firewall Enterprise to Control Center

If you are using Control Center to maintain the TOE configuration, register the firewall with the Control Center. The method you use depends on whether you are using hardware and virtual appliances, or Crossbeam X-Series Platform.

Tasks

- *Hardware and virtual appliances* on page 13
  Register the firewall using the instructions for one of two options for hardware and virtual appliances.
- *Crossbeam X-Series platform* on page 14
  Crossbeam X-Series platforms must be registered to Control Center using the instructions in the installation guide.

Hardware and virtual appliances

Register the firewall using the instructions for one of two options for hardware and virtual appliances.

Tasks

- *One-time passwords are not used* on page 13
  Perform these steps if you have not used one-time passwords.
- *One-time passwords are used* on page 13
  Perform these steps if you have used one-time passwords.

One-time passwords are not used

Perform these steps if you have not used one-time passwords.

Task

1 Register the firewall with Control Center using the information in the *General maintenance* chapter of the product guide, in the *Configure the firewall for other McAfee products* section.

2 Retrieve the configuration from the firewall as detailed in the *Install the Client application* chapter of the Control Center product guide, in the *Add a single firewall* section.

One-time passwords are used

Perform these steps if you have used one-time passwords.

Task

1 At the command prompt, log on to the Firewall Enterprise.

2 Type the following command, then press **Enter**:

```
srole
```

3 Determine if the firewall has been registered to a Control Center. Type the following command, then press **Enter**:

```
cf commandcenter query
```

If there is a Control Center Management Server designated as primary in this output, the firewall must be unregistered. Note the name of the primary server.

4 [Conditional] If the firewall is registered with a Control Center, unregister it. Type the following commands and press **Enter** after each one:

```
cf commandcenter unregister
```

```
cf commandcenter set primary=''
```

```
cf commandcenter delete server=<name>
```

Where *<name>* is the name of the Control Center.

5 Type the following command to add an entry for the Control Center, then press **Enter**:

```
cf commandcenter add server=<name> ipaddr=<ipaddr>
```

where *<name>* is the name of the Control Center and *<ipaddr>* is the IP address of the Control Center Management Server.

6 Type the following command to set the Control Center Management Server as primary, then press **Enter**:

```
cf commandcenter set primary=<name>
```

where *<name>* is the name of the Control Center as defined in the previous step.

7 Type the following command to register with Control Center, then press **Enter**:

```
cf commandcenter register username=<username> password=<password>
```

where *<username>* is an administrative user for the Control Center and *<password>* is the one-time password.

8 Add the firewall to Control Center; see the *Install the Client application* chapter of the Control Center product guide.

Do not select the **Register the firewall with the Management server** checkbox.

Crossbeam X-Series platform

Crossbeam X-Series platforms must be registered to Control Center using the instructions in the installation guide.

Task

1 Download the *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x.

2 Register the firewall using the *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*, version 8.3.x, *Control Center registration* chapter.

Complete the initial setup on a managed firewall

Complete the initial setup, seeing the Control Center product guide as needed.

Task

1. License the firewall. For instructions, see the *Firewall maintenance* chapter of the Control Center product guide, in the *View and manage firewall licenses* section.
2. Configure the zone settings.
3. [All firewalls except Crossbeam X-Series platforms] Add static ARP entries.
   a. At the command prompt, log on to Firewall Enterprise.
   b. Open the /etc/rc.local file for editing.
   c. Add the following line to the end of the /etc/rc.local file for each of the locally attached routers/gateways:

      ```
      arp -s IP_ADDR MAC_ADDR
      ```

      where:

      IP_ADDR = the IP address of the router/gateway

      MAC_ADDR = the MAC address of the router/gateway in the following format:

      xx:xx:xx:xx:xx:xx

      This change creates a static ARP entry for the local routers/gateways.

      

      If the MAC address for any of these IP addresses changes, the respective entries must be updated.

   d. Save your changes and exit.
4. Configure authentication for emergency maintenance mode.
   a. On the command line, log on to Firewall Enterprise.
   b. Open the /etc/ttys file for editing and find this line:

      ```
      console none unknown off secure
      ```

      Change `secure` to `insecure` if not already set as such. This change ensures that administration authentication is required if there is a failure during the boot sequence or when the system starts up to emergency maintenance mode.

   c. Save your changes and exit.
5. Modify the TCP SYN Attack filter.
   a. On the command line, log on to Firewall Enterprise.
   b. Type the following command, then press **Enter**:

      ```
      cf audit mod filter name="TCP SYN Attack" sacap_filter="event
      AUDIT_R_NET_TCP_SYNATTACK && ! src_ip IP_ADDR/32" number=11 filter_type=attack
      ```

      where *IP_ADDR* is the IP address of the default gateway for Firewall Enterprise.

   c. Start the Control Center Client application and log on to the Control Center Management Server.
   d. In the navigation pane, select **Policy**.

e In the **Policy** tree, expand the **Firewalls** node.

f Right-click the firewall you are configuring for the TOE, and select **Retrieve Firewall Objects**. The **Firewall Retrieval Options** window is displayed.

g Select **Audits and Alerts**.

h Click **OK**. The **System Update** window appears.

i Click **Yes**.

This change prevents your default gateway IP address from triggering a TCP SYN Attack filter.

6 Use the Control Center Client application to set the IP network defense.

a In the navigation pane, select **Policy**.

b In the lower left area of the window, click the **Firewall Settings** tab.

c Expand the **Network Defenses** node.

d Double-click the network defense object used by the firewall you are configuring for the TOE. The **Network Defenses** window appears.

e Click the **IP** tab.

f If it is not already enabled, select **source broadcast address** and **incorrect source address for interface**.

g Click **OK**.

h Apply the changes to the firewall.

7 Make sure that the authentication failure lockout options are configured with the necessary integer limit on the external authentication servers.

Use the Control Center Client application to configure external authentication servers. See the *Control Center settings* chapter of the Control Center product guide for instructions.

8 Create a configuration backup. See the *Firewall maintenance* chapter of the Control Center product guide for instructions.

9 Disable or remove any rules allowing command line access. The command line interface cannot be used to maintain a TOE configuration.

Configure password requirements on a managed firewall

Configure the password requirements as described in *Create your password*.

Even though Firewall Enterprise might support additional characters, select only from the designated set of 94 characters.

Follow these steps to configure your password.

Task

For option definitions, press **F1** or click **Help** in the interface.

1 From the Control Center Client application, select **Policy** | **Rule Objects** | **Authenticators**.

2 Expand the **Password Authenticators** node.

3 Double-click the **Password Authenticator** object used by the firewall you are configuring for the TOE.

The **Password Authenticator** window appears.

4 In the **Minimum Password Length** field, enter `12`.

5 Select the **Require complex passwords** option and enter the following values:

- In the **Required number of character groups** field, enter `3`.
- In the **Required number of characters per character group** field, enter `1`.

There might be a delay in the password expiration. Do not rely on this setting.

6 Click **OK**.

7 Apply the changes to the firewall.

8 If using external authentication, authentication failure lockout handling must be set on external authentication servers such as RADIUS, LDAP, and Microsoft Windows Domain.

See also

Create your password on page 4

Maintaining a TOE configuration

Follow these guidelines to use each chapter of the product guide to configure and maintain Firewall Enterprise in a manner that meets the TOE configuration. By default, almost all features and services are set to deny, off, or disabled during the initial configuration.

Use the following descriptions of each chapter as guidelines for which services and features can be enabled in a TOE configuration. These guidelines are most often exceptions to the instructions written in the product guide. If a feature or service is listed, configure the mentioned item as described therein. This section is structured in the same manner as the product guide, as if administered using the Admin Console, but is equally applicable to administration using Control Center.

Before reading the corresponding chapter in the product guide, read the guidelines for each chapter listed.

Chapter	Configuration
Introduction	
Chapter 1: Introduction to Firewall Enterprise	All necessary configuration takes place during the installation and configuration process detailed earlier in this document. Do not update the Firewall Enterprise software using the Admin Console's **Software Management** area.
Chapter 2: Planning	All necessary configuration takes place during the installation and configuration process detailed earlier in this document.
Chapter 3: Installation and configuration	Use the Admin Console for administration. The local console and remote administration using Secure Shell (SSH) or Telnet are not permitted in a TOE configuration. All remote administration from external networks is prohibited.
Chapter 4: Startup	After the initial configuration has been completed, the command line interface must be disabled and the Admin Console or Control Center must be used for all administrative tasks.
Policy	
Chapter 5: Policy overview	Follow these guidelines for the TOE configuration.
Chapter 6: Network objects and time periods	Follow these guidelines for the TOE configuration.

Chapter	Configuration
Chapter 7: Identity validation	• Set up authentication for network connections, including the Admin Console. • Select strong authentication (one-time password) through an external authentication server when setting up authentication for Telnet or FTP sessions. Telnet and FTP sessions do not use the Telnet and FTP servers. Sessions allow traffic through the firewall, whereas servers allow traffic to the firewall. • Do not configure Passport authentication, and do not allow users to change their own passwords.
Chapter 8: Content inspection	The content inspection services described in this chapter are not supported in a TOE configuration and should not be enabled.
Chapter 9: Endpoint Intelligence Agent	Follow these guidelines for the TOE configuration.
Chapter 10: Applications	Follow these guidelines for the TOE configuration.
Chapter 11: Application Defenses	Configure Application Defenses that are appropriate for your site-specific security policy. Remember that the Application Defenses should only be used for the various proxy services that are included in the evaluated configuration.
Chapter 12: Access control rules	Create rules that are appropriate for your site-specific security policy. Remember that the rules can only use the various services that are included in the evaluated configuration. Packet Filter services are allowed as documented in the product guide.
Chapter 13: SSL rules	Follow these guidelines for the TOE configuration.
Chapter 14: Policy in action	Follow these guidelines for the TOE configuration.
Monitoring	
Chapter 15: Dashboard	Follow these guidelines for the TOE configuration.
Chapter 16: Auditing	Firewall Enterprise acts to limit audit data loss. It is preconfigured to monitor the audit logs to prevent auditable events, except those taken by the authorized administrator in the event the audit log is full. The administrator should always leave the block_unaudited_actions feature enabled; this setting stops the flow of data through the firewall when the audit log becomes full. These actions are implemented with the Firewall Enterprise logcheck facility. Read the logcheck man page for information about logcheck operations. The logcheck /secureos/etc/logcheck.conf configuration file can be edited to change the thresholds for action. The overwrite_old_logfiles parameter in the logcheck.conf file dictates whether to delete the oldest audit archive on the log partition when the partition is full.
Chapter 17: Audit responses	Follow these guidelines for the TOE configuration.
Chapter 18: ePolicy Orchestrator integration	ePolicy Orchestrator is not supported in a TOE configuration and should not be enabled.

Chapter	Configuration
Chapter 19: Network defenses	Enable any of the network defenses, but do not disable any, including **source broadcast address** and **incorrect source address for interface** that have been specifically enabled by this document. **Disabling Network Defenses** only disables the auditing of the event; Firewall Enterprise always blocks the attacks.
Chapter 20: SNMP	The SNMP agent is not supported in a TOE configuration and should not be enabled.
Networking	
Chapter 21: IPv4 and IPv6 overview	Follow these guidelines for the TOE configuration.
Chapter 22: Security zones	Follow these guidelines for the TOE configuration.
Chapter 23: Interfaces and NICs	Follow these guidelines for the TOE configuration.
Chapter 24: Quality of Service	Follow these guidelines for the TOE configuration.
Chapter 25: DHCP Relay	Follow these guidelines for the TOE configuration.
Chapter 26: Routing	Dynamic routing is not supported in a TOE configuration and should not be enabled. Use only static routing.
Chapter 27: DNS (domain name system)	Firewall-hosted DNS services, including DNSSEC, are not supported in a TOE configuration and should not be enabled. Transparent DNS services are allowed as documented in the product guide.
Chapter 28: Email	Follow these guidelines for the TOE configuration.
Chapter 29: VPN (virtual private networks)	Follow these guidelines for the TOE configuration.
Maintenance	
Chapter 30: Administration management	The evaluated configuration allows for management by either the Admin Console or Firewall Enterprise Control Center. The command line interface must not be used.
Chapter 31: General maintenance	If Firewall Enterprise is required to maintain an evaluated configuration, the administrator can only install a patch that has passed the necessary evaluation requirements to maintain the certification. FIPS 140-2 validated mode must be enforced. Take appropriate steps to safeguard any configuration backup files against unauthorized access, and consider using the optional encryption feature as an extra protective measure.
Chapter 32: Certificate/key management	Follow these guidelines for the TOE configuration.
Chapter 33: High Availability	High Availability is not supported in a TOE configuration and should not be enabled.
Troubleshooting	
Appendix A: Troubleshooting	Follow these guidelines for the TOE configuration.
Appendix B: Reinstallation and recovery options	If you reinstall, the procedure in *Install and configure Firewall Enterprise* must be reapplied.

Registering TOE users

Customers have the option to register people within their organization as TOE users who automatically receive information and fixes related to TOE security flaws in a timely manner. McAfee Customer Service is the official point of contact for TOE security issues and TOE user registration.

To register a TOE user, call McAfee Customer Service and provide the necessary contact information. See mysupport.mcafee.com for Customer Service contact information.

Report an issue

After installing Firewall Enterprise and setting it up to meet the TOE configuration, the firewall is expected to perform as configured and function well. If you suspect a security flaw with a firewall in the TOE configuration, report it to McAfee, Inc., for resolution.

Use the flaw remediation process to report and resolve a potential security flaw in the TOE.

Task

1 Ensure the following prerequisites are met:

- McAfee Firewall Enterprise must be currently licensed for support.
- McAfee Firewall Enterprise must be running in a Common Criteria-evaluated configuration.

2 Report the suspected security flaw.

Contact McAfee, Inc., technical support (mysupport.mcafee.com) and report the suspected security flaw. Notify technical support that the firewall is installed in the Common Criteria TOE configuration.

In the case of a configuration problem, the report of the suspected security flaw will be entered into the flaw remediation database, the technical support database, or both for subsequent resolution.

In addition to reporting the suspected security flaw, you can request correction and inquire about the status of the flaw.

3 Obtain a flaw remedy from the McAfee support team.

The McAfee, Inc., engineering or technical support department, or both, will review the report of the suspected security flaw and identify a remedy to the flaw as appropriate. You will be notified of any corrective action taken as a result of the report.

Customer Service can also be contacted to report flaws, obtain flaw reports, or to inquire about security issues involving the TOE.