Common Criteria Evaluated Configuration Guide

McAfee® Firewall Enterprise (*Sidewinder*®)

version 7.0.1.03

About this Guide

This guide describes requirements and guidelines for installing, configuring, and maintaining a McAfee® Firewall Enterprise (*Sidewinder*®) appliance to comply with Common Criteria (CC) evaluation standards. If your company security policy requires your Firewall Enterprise appliance to exactly match the CC Target of Evaluation (TOE) configuration, carefully follow the instructions in this document.

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 (CC) certified. The McAfee® Firewall Enterprise (Sidewinder®) appliance and software version 7.0.1.03 have 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, McAfee, Inc., refers to McAfee® Firewall Enterprise in the evaluated configuration as the Target of Evaluation (TOE). References to the TOE configuration imply that McAfee Firewall Enterprise is installed and configured as described in the *McAfee Firewall Enterprise Security Target* document.

This document explains how to install and use the TOE configuration. This document applies to the McAfee Firewall Enterprise appliances and software version 7.0.1.03.

Using the *Common Criteria Evaluated Configuration Guide*

To plan and implement a TOE configuration, use this document (also referred to as the configuration guide) to supplement the following documents:

- *McAfee Firewall Enterprise (Sidewinder) Setup Guide*, version 7.0.1.02
- *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03
- *McAfee Firewall Enterprise (Sidewinder), Virtual Appliance Product Guide*, version 7.0.1.02
- *McAfee Firewall Enterprise (Sidewinder) on Riverbed Services Platform Installation Guide*, version 7.0.1.02

To maintain the TOE configuration, use this document to supplement the following document:

- *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03

These documents provide information about all of the firewall's services, features, and navigation, in addition to general networking concepts. The configuration guide states the parameters and requirements for setting up and maintaining a Firewall Enterprise run in a CC-evaluated configuration.

Reference material

See the following for more information on Common Criteria, McAfee, Inc., and McAfee Firewall Enterprise and its evaluation level requirements:

- http://www.commoncriteriaportal.org
- mysupport.mcafee.com

Security objectives for the environment

The TOE is assured to provide effective security measures in a cooperative, non-hostile environment when correctly installed and managed. Ensure that the TOE environment meets the necessary security objectives. The environment for the TOE should be managed to satisfy the assumptions stated in the *McAfee Firewall Enterprise Security Target* document.

TOE security environment considerations

The TOE environment needs to be established and managed to meet the following physical and logical constraints:

- The configured TOE shall manage traffic for at least two (2) networks, at least one of which is designated as internal and one is designated as external.
- The configured TOE shall also support a separate network interface that is used exclusively for communications between the TOE and an administration workstation and the single-use authentication mechanism.
- The administrators can manage TOE remotely as well.
- 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 SafeWord PremierAccess or 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 device shall be controlled along with the TOE and the network link connecting them.

Verify secure delivery of a Firewall Enterprise appliance

This section provides information on ensuring the secure delivery of the McAfee Firewall Enterprise security appliances.

Use the following steps to ensure that the correct appliance model has been received:

1. Examine the outside packaging and markings of the delivery container 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 Firewall Enterprise 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, since 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.

   Download the correct installation media from the McAfee Technical Support Service Portal using the procedure, *Download 7.0.1.02 installation media*.

Configuring password authentication in a TOE configuration

Strong passwords are a vital part of ensuring network security. The guidance in this section applies to creating and managing McAfee Firewall Enterprise administrator and user passwords as a supplement to the password guidance included in the *McAfee Firewall Enterprise (Sidewinder) Setup Guide* (also referred to as the setup guide) and *McAfee Firewall Enterprise (Sidewinder) Administration Guide (*also referred to as the administration guide).

Password recommendations

Ensure 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 McAfee Firewall Enterprise run in a CC-evaluated configuration supports passwords created from letters, numbers, and special characters. The following characters can always be used in a password:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ

abcdefghijklmnopqrstuvwxyz

1234567890

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

Configure the password requirements

The administrator should only select from the designated set of 94 characters when forming a password, even though McAfee Firewall Enterprise might support additional characters. A keyboard that provides the 94 characters is required for the TOE, for example, a U.S. keyboard.

Follow these steps to configure the password requirements.

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

2 Click **Password** and go to the General tab.

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

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**.

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

Set up a TOE configuration

To set up a TOE configuration, first re-image the firewall to version 7.0.1.02. Follow the guidelines to set up a TOE configuration on a Firewall Enterprise physical appliance or virtual appliance or on the Riverbed services platform. After setting up these, follow the steps to upgrade to version 7.0.1.03.

Re-image to version 7.0.1.02

Download and validate the 7.0.1.02HW04 installation media, and then re-image the firewall to 7.0.1.02HW04.

- *Download 7.0.1.02 installation media*
- *Validate the image files*
- *Create installation media*
- *Install version 7.0.1.02*

Note: Follow these instructions for Firewall Enterprise physical and virtual appliances. Use these steps even for Firewall Enterprise on the Riverbed Services Platform.

Download 7.0.1.02 installation media

1 Download the 7.0.1.02HW04 installation media.

a Visit www.mcafee.com/us/downloads.

b Provide your grant number, then navigate to the appropriate product and version.

Tip: Your grant number is included in the grant letter you received from McAfee.

c Determine whether you need a CD or USB image.

d Make a note of the MD5 signature in the Notes column. You will use this signature later to validate the downloaded software to the local MD5 signature.

e Navigate to the .iso or USB.zip file, and download it on your system.

2 Download the 7.0.1.02 Admin Console installation media.

Note: Download the Admin Console only for the CD-based McAfee Firewall installation image. The Firewall Enterprise 7.01.02HW04 USB image includes the Admin Console installation.

a Visit www.mcafee.com/us/downloads.

b Provide your grant number, then navigate to the appropriate Admin Console version.

c Make a note of the MD5 signature for the image file.

d Download the .iso file on your system.

Validate the image files

Perform an MD5 signature validation for the downloaded image files.

Using an MD5 signature generation tool, such as *WinMD5 Sum*, generate an MD5 signature and compare it to the MD5 signature noted in the preceding section. The signatures must match.

Note: If the signatures do not match, contact technical support for assistance.

Examples of how to generate MD5 signatures for an .iso image file:

- md5 <filename>
- md5sum <filename>

Create installation media

Create installation media from the validated image files.

- For CD installation media, use CD-burning software (such as Nero or Roxio) to burn CDs from the .iso files.
- For USB installation media, unzip the USB.zip file and use software (such as Image Writer) to write the .usb file to an USB drive.

Install version 7.0.1.02

Re-image the firewall to 7.0.1.02HW04.

- **Firewall Enterprise physical appliance —** Follow the instructions in *Appendix B* of the administration guide.
- **Firewall Enterprise, Virtual Appliance —** Follow the instructions in *Re-installing* of the *Virtual Appliance Product Guide*.
- **Firewall Enterprise on Riverbed Services Platform —** Follow the instructions from the *Riverbed Services Platform Installation Guide*.

Set up a TOE configuration for a Firewall Enterprise physical appliance

This section provides guidelines for using each chapter of the setup guide to set up McAfee Firewall Enterprise in a manner that meets the TOE configuration. These guidelines and requirements are most often exceptions to the instructions written in the setup guide. If a feature or service is listed below, you must configure the mentioned item as described in this section. If a feature or service is not listed below, configure it as written in the setup guide.

Tip: Before reading the corresponding chapter in the setup guide, read the guidelines for each chapter listed below.

Pre-installation tasks

Chapter 1: Planning your McAfee Firewall Enterprise Setup

Review the high-level steps to get the Firewall Enterprise up and running. The following general configuration rules should be kept in mind at this time:

- Install version 7.0.1.02HW04 software using either the *Installation — Disk Imaging* CD or USB drive. Follow the instructions in *Appendix B* of the administration guide.

  Even though *Appendix B* goes over re-imaging an appliance, the instructions also apply to a new TOE software installation.

  Note: The firewall will be upgraded to version 7.0.1.03 at a later stage.

- In the case of appliance model TOE versions, the pre-loaded software scenario does not apply.
- A local console (keyboard and monitor, or serial terminal) is required only when installing the Firewall Enterprise software.

Prepare for integrating McAfee Firewall Enterprise into your network. While creating your installation plan, incorporate the following special requirements:

- Follow the guidance in *Configuring password authentication in a TOE configuration* when selecting the initial administration user password.
- Plan to use two network interfaces for managed traffic: one for an internal burb and one for an external burb.
- Also plan to use a third network interface for an administrative burb. This network interface will connect McAfee Firewall Enterprise to the administrator workstation and to the authentication server.
- Plan for a transparent DNS configuration.
- Plan for transparent SMTP services.
- Plan for the *Allow administrative services only* feature instead of enabling the *Allow administrative and basic outbound Internet services* feature. This prohibits non-administrative traffic.
- Plan for remote administration on the internal burb to begin with. After all configuration steps are complete, administration only takes place on the administrative burb.
- Activate a BIOS password on the appliance.

Chapter 2: Installing the Management Tools

Follow the instructions in Chapter 3 to set up the administration software, Admin Console, on a Windows-based computer.

Installation tasks

Chapter 3: Configuring Your McAfee Firewall Enterprise

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

- Connect a network cable for the third administrative network interface.
- Select **Create Configuration**.

- Select **Allow administrative services only**.
- Do not enter a remote administration route because the Admin Console must be locally attached to the internal burb. It will be moved to the administrative burb later.
- [Conditional] If you select the **Save Configuration** option, you must maintain the security of the saved configuration.

  Tip: 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 the upgrade package using the instructions in *Upgrade to version 7.0.1.03*.

Chapter 4: Managing Your McAfee Firewall Enterprise

At this point, the McAfee Firewall Enterprise software is loaded and the initial configuration (from the Quick Start Wizard) is in place and ready for administration on the internal network. Follow these instructions referring to the procedures in the setup guide and administration guide when instructed.

Note: The total evaluated configuration for the TOE will require some additional actions to switch the administration over to the separate administrative network.

1. Configure an administrative Windows-based workstation on the internal network and follow the instructions in Chapter 5 of the setup guide for starting the Admin Console on this workstation.
2. Check for license activation as instructed for an isolated firewall.
3. Configure the burb settings.
   a. Add the administrative burb.
   b. Configure a third interface on the administrative burb.
   c. Change the Admin Console rule to allow access from the administrative burb and not from the internal burb.
   d. Restart the firewall and move the administrative Windows-based workstation to the administrative burb network.
   e. Restart the Admin Console. See “Starting the Admin Console” in Chapter 5 of the setup guide for instructions.
4. 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

   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= the IP address of the default gateway for McAfee Firewall Enterprise.

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 ensures that administration authentication is required if there is a failure during the boot sequence or when the system boots to Emergency Maintenance Mode.

5 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**.

6 Activate the authentication failure lockout option and enter the desired integer limit. See Chapter 5 of the administration guide for instructions.

7 At this point, the administrator should create a configuration backup. See Chapter 21 of the administration guide for instructions.

8 Use the information in the "Performing other post-startup tasks" section of the setup guide's Chapter 5 for reference only. All of these additional tasks can only be done to the extent that they comply with the instructions in *Maintain a TOE configuration* section of this document.

Set up a TOE configuration for a Firewall Enterprise virtual appliance

This section provides guidelines for using each chapter of the *McAfee Firewall Enterprise (Sidewinder), Virtual Appliance Product Guide* to set up the McAfee Firewall Enterprise, Virtual Appliance in a manner that meets the TOE configuration.

Note: After setting up the 7.0.1.02 virtual firewall, upgrade the virtual firewall to 7.0.1.03. Refer to the section, *Upgrade to version 7.0.1.03*.

Chapter 1: About McAfee Firewall Enterprise, Virtual Appliance

This chapter explains the hardware and software requirements for setting up a virtual firewall, and deployment scenarios to protect the virtual machines are also explained.

Chapter 2: Prepare your ESX server

This chapter explains configuring the ESX virtual networking and the Network Time Protocol (NTP).

Chapter 3: Setup the McAfee Firewall Enterprise, Virtual Appliance

This chapter explains how to set up and configure the virtual firewall and the ESX server.

Chapter 4: Set Up Administrative Access

This chapter explains the procedures to install the Firewall Enterprise Admin Console, log on to the virtual firewall using the Admin Console, and manually activate the virtual firewall's license.

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 4.0 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 burb network as the Admin Console.

Set up a TOE configuration for a Firewall Enterprise on a Riverbed Services Platform

Follow these guidelines for using each chapter of the *McAfee Firewall Enterprise (Sidewinder) on Riverbed Services Platform Installation Guide* to set up the McAfee Firewall Enterprise on the Riverbed Services Platform to meet the TOE configuration.

Chapter 1: Introduction

This chapter explains the requirements to run Firewall Enterprise on Riverbed Steelhead appliances and provides deployment scenarios that protect the WAN traffic.

Chapter 2: Firewall Installation

This chapter provides steps to install Firewall Enterprise on the Riverbed Services Platform. It helps you to deploy the firewall as an in-band WAN package.

Chapter 3: Setup

This chapter explains the setting up of the firewall and the Admin Console. It also provides details on how to configure policies and do post-setup tasks.

Upgrade to version 7.0.1.03

After you have set up Firewall Enterprise on a physical or virtual appliance or on the Riverbed Services Platform, upgrade the software to version 7.0.1.03.

Download, validate, and install the 7.0.1.03 patch to upgrade to 7.0.1.03.

- *Download the 7.0.1.03 patch*
- *Validate the 7.0.1.03 patch*
- *Install the 7.0.1.03 package*

Download the 7.0.1.03 patch

Use a web browser to download the 7.0.1.03 package, then manually load the package on the firewall.

1. Go to go.mcafee.com/goto/updates.
2. Scroll down to the McAfee Firewall Enterprise Upgrades and Patches entry for version 7.0.1.03, then click **Download.**
3. Enter a valid Firewall Enterprise serial number, then click **Submit.**
4. Make a note of the MD5 signature for the image file.
5. Click **Download Patch** for version 7.0.1.03.

Validate the 7.0.1.03 patch

Perform an MD5 signature validation for the downloaded patch.

Using an MD5 signature generation tool, such as *WinMD5 Sum*, generate an MD5 signature and compare it to the MD5 signature noted in the preceding section. The signatures must match.

Note: If the signatures do not match, contact technical support for assistance.

Install the 7.0.1.03 package

Follow these steps to install the 7.0.1.03 package.

1. Copy the 70103 patch file to an internal FTP server accessible from the firewall.
2. At the McAfee Firewall Enterprise local console, FTP the 70103 patch file to the firewall.
3. At the McAfee Firewall Enterprise local console, enter the following command to load the patch:

   ```
   cf package load packages=70103 source=file
   ```

4. At the McAfee Firewall Enterprise local console, enter the following command to install the patch.

   ```
   cf package install packages=70103
   ```

For further instructions, refer to *McAfee Firewall Enterprise (Sidewinder) Release Notes*, version 7.0.1.03. Follow these sections of the Release notes:

- Update the Admin Console
- Verify that version 7.0.1.03 is installed

Maintain a TOE configuration

This section provides guidelines and requirements for using each chapter of the administration guide to configure and maintain McAfee 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 administration guide. If a feature or service is listed below, you must configure the mentioned item as described therein.

Tip: Before reading the corresponding chapter in the administration guide, read the guidelines for each chapter listed below.

Introduction

Chapter 1: Introduction to McAfee Firewall Enterprise

All necessary configuration takes place during the installation and configuration process detailed earlier in this document.

Do not update the McAfee Firewall Enterprise software using the Admin Console's Software Management area.

Chapter 2: Administrator Basics

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.

Note: When the initial configuration has been completed, the command line interface should be disabled and the Admin Console should be used for all administrative tasks.

Policy

Chapter 3: Policy Configuration Overview

This chapter explains how policy rules are configured.

Chapter 4: Network Objects and Time Periods

This chapter explains network objects and time periods. Network objects and time periods can be used in an evaluated configuration.

Chapter 5: Authentication

This chapter explains authentication. Note the following guidelines and requirements:

- Set up authentication for network connections, including Admin Console.
- Select a strong authentication (one-time password) service such as SafeWord when setting up authentication for Telnet or FTP sessions.

Note: 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 6: Content Inspection

Do not configure any of the content inspection services described in this chapter.

Chapter 7: Services

This chapter explains services on McAfee Firewall Enterprise.

Chapter 8: Application Defenses

This chapter explains Application Defenses. Administrators can configure Application Defense that are appropriate for their site-specific security policy. Remember the Application Defenses should only be used for the various proxy services that are included in the evaluated configuration.

Chapter 9: Rules

This chapter explains the rules. Administrators can create rules that are appropriate for their site-specific security policy. Remember the rules can only make use of the various services that are included in the evaluated configuration. Packet Filter services are allowed as documented in the administration guide.

Monitoring

The administrator can monitor McAfee Firewall Enterprise using the facilities available through the Admin Console.

Chapter 10: The Dashboard

This chapter explains the McAfee Firewall Enterprise dashboard.

Chapter 11: Auditing

This chapter explains auditing and reporting on the McAfee Firewall Enterprise.

McAfee Firewall Enterprise takes actions 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 stops the flow of data through the firewall when the audit log becomes full. These actions are implemented by means of the McAfee Firewall Enterprise logcheck facility.

The administrator is directed to read the logcheck man page for information about the logcheck operation. The administrator can read the */secureos/etc/logcheck.conf* file for additional guidance, as well as other adjustable logcheck settings. The logcheck configuration file can be edited to change the thresholds for action.

Chapter 12: Service Status

This chapter explains how services are controlled on McAfee Firewall Enterprise.

Chapter 13: IPS Attack and System Event Responses

This chapter explains event responses.

Chapter 14: Network Defenses

This chapter explains Network Defenses. Administrators can enable any of the Network Defenses but must 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; McAfee Firewall Enterprise always blocks the attacks.

Chapter 15: The SNMP Agent

Do not configure the SNMP agent.

Networking

Chapter 16: Burbs Interfaces, and Quality of Service

This chapter explains McAfee Firewall Enterprise burbs and interfaces.

McAfee Firewall Enterprise must be configured with three burbs to be in conformance with the evaluated configuration. One burb each for the internal and external (Internet) networks and a third burb for administration and authentication.

Chapter 17: Routing

Do not configure any dynamic routing on McAfee Firewall Enterprise. Use only static routing.

Chapter 18: DNS (Domain Name System)

Transparent DNS services are allowed as documented in the administration guide. Do not configure firewall-hosted DNS services.

Chapter 19: E-Mail

Do not configure electronic mail using Sendmail servers or mail filters. Configure transparent mail using the SMTP proxy instead.

Chapter 20: Virtual Private Networks

Configure VPNs according to this chapter and your site security policy.

Maintenance

Chapter 21: General Maintenance Tasks

This chapter explains the basic maintenance tasks on McAfee Firewall Enterprise. If McAfee 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.

Note: FIPS must be enforced.

Take appropriate steps to safeguard any configuration backup files against unauthorized access, and consider using the optional encryption feature as an additional protective measure.

Chapter 22: Certificate/Key Management

This chapter explains the certificate and key management.

Certificates are used to verify the identity and authenticity of hosts. Certificates are used along with keys to secure communication.

Chapter 23: High Availability

Do not configure High Availability.

Troubleshooting

Appendix A: Basic Troubleshooting

This appendix contains useful information but is not required for running the McAfee Firewall Enterprise in the evaluated configuration.

Appendix B: Re-install and Recovery Options

This appendix provides the re-installation and recovery options for McAfee Firewall Enterprise. In the event of a re-installation the procedure in *Set up a TOE configuration for a Firewall Enterprise physical appliance* should be re-applied.

Flaw remediation guidance

After installing the Firewall Enterprise and setting it up to meet the TOE configuration, the firewall is expected to perform as configured and function well. An administrator can report a suspected security flaw with a firewall in the TOE configuration to McAfee, Inc., for resolution. The following is an outline of the steps taken to report and resolve potential security flaws in the TOE:

1. Ensure the following prerequisites are met.
   - McAfee Firewall Enterprise must be currently licensed for support.
   - McAfee Firewall Enterprise must be in running in a CC-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 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. The customer will be notified of any corrective action taken as a result of the customer report made by the customer.
4. Contact the McAfee Customer Service to register 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. Customer Service can also be contacted to report flaws, obtain flaw reports, or to inquire about security issues involving the TOE. See mysupport.mcafee.com for contact information.