Configuration Guide

FIPS 140-2

McAfee Firewall Enterprise (*Sidewinder*)

version 7.0.1.03

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

License Attributions

For information about license attributions, see **Help | About** in the McAfee® Firewall Enterprise Admin Console.

Contents

About this document 5

1 Introduction to FIPS 140-2 7

About FIPS 140-2 on Firewall Enterprise . . . 7
Steps to make Firewall Enterprise FIPS 140-2 compliant . . . 7
Requirements . . . 8

2 Install version 7.0.1.03 9

About installing patch 7.0.1.03 . . . 9
Install version 7.0.1.02 . . . 9
Procedure 1 — Create a configuration backup . . . 9
Procedure 2 — Download version 7.0.1.02 files . . . 9
Procedure 3 — Install version 7.0.1.02 package . . . 10
Procedure 4 — Upgrade to version 7.0.1.03 . . . 10
Prepare the appliance for FIPS 140-2 Level 2 compliance . . . 10

3 Enable FIPS 140-2 processing 11

Enabling FIPS 140-2 processing . . . 11
Enable FIPS 140-2 processing using the Admin Console . . . 11
Enable FIPS 140-2 processing using the command line . . . 11
Troubleshooting . . . 11

4 Update and v erify configurations 13

Replace critical security parameters . . . 13
Replacing certificates . . . 14
Verify allowed cryptographic services . . . 16
Verify approved cryptographic algorithms and key lengths . . . 16
Certificate authorities and remote certificates . . . 17
IPsec and IKE . . . 17
Verify SSH client and server configurations . . . 18
Restrict administrator access . . . 18
Verify SNMP version 3 configurations . . . 18
Add or modify an SNMP v3 user . . . 18
Verify the trap user configuration . . . 19

5 Leave FIPS mode 21

About this document

Use this guide to make a McAfee® Firewall Enterprise (Sidewinder®) (hereinafter Firewall Enterprise) compliant with FIPS 140-2 standards. This guide includes procedures for hardware modifications, software updates, and configuration changes that meet security requirements for cryptographic modules.

This guide is intended for network and security administrators. It assumes familiarity with UNIX and Windows operating systems, system administration, the Internet, networks, and related terminology.

Certification information

McAfee, Inc. products running version 7.0.1.03 meet FIPS 140-2 security requirements.

The security policies and validation certificates can be viewed at the NIST web site:

csrc.nist.gov/groups/STM/cmvp/validation.html.

Additional information

You can find additional information at the following locations:

- **Documentation** — Product manuals, configuration-specific application notes, and the KnowledgeBase are available at mysupport.mcafee.com.
- **Online Help** — Online Help is built into Firewall Enterprise. Click the **Help** button or ? icon located on any window.

1 Introduction to FIPS 140-2

Contents

About FIPS 140-2 on Firewall Enterprise

Steps to make Firewall Enterprise FIPS 140-2 compliant

Requirements

About FIPS 140-2 on Firewall Enterprise

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to promote the use of validated cryptographic modules and provide Federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

McAfee® Firewall Enterprise (Sidewinder®) (hereinafter Firewall Enterprise) models have been validated as a cryptographic module at the platform level. The McAfee Firewall Enterprise Cryptographic Module provides FIPS 140-2-compliant cryptographic services on Firewall Enterprise version 7.0.1.03. These services include symmetric key encryption and decryption, public key cryptography, hashing, and random number generation.

The FIPS 140-2 standard provides various increasing levels of security.

- Firewall Enterprise version 7.0.1.03 hardware appliances (with the addition of a FIPS kit) are certified to Level 2.
- Firewall Enterprise version 7.0.1.03 low-end appliances and virtual appliances, are certified to Level 1.

Steps to make Firewall Enterprise FIPS 140-2 compliant

FIPS 140-2 validated mode (hereinafter FIPS mode) is a separate operational state for Firewall Enterprise. Hardware modifications, a software update, and configuration changes are necessary to put your firewall in FIPS mode and make it compliant with FIPS 140-2 requirements. Follow the instructions in this guide to perform the following actions:

- Install patch 7.0.1.03.
- [FIPS 140-2 Level 2 only] Prepare the appliance. See the *McAfee Firewall Enterprise FIPS Kit Installation Guide* for your appliance model.
- Enable FIPS 140-2 processing and restart the firewall.
- Verify compliance.
  - Replace critical security parameters.
  - Verify allowed cryptographic services.
  - Verify approved cryptographic algorithms.
  - Restrict administrator access.

Requirements

To make Firewall Enterprise compliant with FIPS mode, you need the following:

- One of the following firewall types:
  - McAfee Firewall Enterprise appliance
  - McAfee Firewall Enterprise, Virtual Appliance
- [FIPS 140-2 Level 2 only] The FIPS 140-2 kit containing security baffles (that is, there could be more than one in a particular FIPS kit, depending on how many openings need to be covered) and/or tamper-evident stickers.

2 Install version 7.0.1.03

Contents

About installing patch 7.0.1.03

Install version 7.0.1.02

Prepare the appliance for FIPS 140-2 Level 2 compliance

About installing patch 7.0.1.03

To be FIPS 140-2 compliant, your Firewall Enterprise appliance must be running version 7.0.1.03 when you enable FIPS mode and update your firewall configuration. You must have version 7.0.1.02 installed before you can upgrade to version 7.0.1.03.

If your firewall is managed by McAfee® Firewall Enterprise Control Center (hereinafter Control Center), refer to the *McAfee Firewall Enterprise Control Center Product Guide* for instructions.

Install version 7.0.1.02

Use the following procedures to install version 7.0.1.02 and upgrade to version 7.0.1.03:

- If you firewall is already at version 7.0.1.02, go to *Procedure 4 — Upgrade to version 7.0.1.03*
- If you have a newly purchased Firewall Enterprise with version 7.0.1.00, you must perform the initial configuration before proceeding.

Procedure 1 — Create a configuration backup

McAfee recommends that you create a configuration backup before upgrading. Backing up the configuration files lets you quickly restore a firewall.

For instructions on creating a configuration backup, refer to the *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03.

Procedure 2 — Download version 7.0.1.02 files

Perform this procedure to download the version 7.0.1.02 files.

1. In a web browser, navigate to www.mcafee.com/us/downloads.
2. Provide your grant number, then navigate to the appropriate product and version.
3. Download the appropriate files.
   - **Management Tools** — Download the McAfee Firewall Enterprise Admin Console executable (.exe) file or CD image (.iso) file.

     Tip: Select the CD image file if you want to create a CD for use in installing the Management Tools.
   - **Version 7.0.1.02 image** — Download the installation image.

     Tip: Select the USB image file if your appliance does not have a CD-ROM drive.

4 Create physical installation media using the downloaded installation files.

- Write the .iso file(s) to a CD.

  Note: If you downloaded multiple .iso files, use a separate CD for each file.

- If you downloaded the USB image file, write the image to a USB drive. Refer to KnowledgeBase article **KB69115** for instructions.

Procedure 3 — Install version 7.0.1.02 package

Refer to the appropriate installation instructions for your appliance:

- *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.02
- *McAfee Firewall Enterprise, Virtual Appliance Product Guide*, version 7.0.1.02

Procedure 4 — Upgrade to version 7.0.1.03

Upgrade the version 7.0.1.02 firewall to 7.0.1.03. See the *McAfee Firewall Enterprise (Sidewinder) Release Notes*, version 7.0.1.03*,* for upgrade instructions.

Prepare the appliance for FIPS 140-2 Level 2 compliance

To achieve FIPS 140-2 Level 2 compliance for your appliance, install the FIPS kit before proceeding to the next chapter. For instructions, see the McAfee Firewall Enterprise FIPS Kit installation guide for your appliance.

Note: The FIPS kit is not required to achieve FIPS 140-2 Level 1 compliance.

3 Enable FIPS 140-2 processing

Contents

Enabling FIPS 140-2 processing

Troubleshooting

Enabling FIPS 140-2 processing

You can enable FIPS 140-2 processing on Firewall Enterprise using either the Admin Console or the command line.

Note: The firewall must be restarted to activate the change.

Enable FIPS 140-2 processing using the Admin Console

1. Select **Maintenance | FIPS**. The FIPS check box appears in the right pane.
2. Select **Enforce US Federal Information Processing Standard 140-2**.
3. Save the configuration change.
4. Select **Maintenance | System Shutdown** and restart the firewall to activate the configuration change.

Enable FIPS 140-2 processing using the command line

1. Enter the following command:

   ```
   cf fips set enabled=1
   ```

   See the cf_fips man page for more information.
2. After the command completes, restart the firewall to activate the configuration change:

   ```
   shutdown -r now
   ```

Troubleshooting

- If FIPS 140-2 processing was successfully enabled, an audit message will be generated after the firewall is restarted. Here is an example of this audit:

  ```
  Dec  5 16:31:42 2008 EST  f_system a_general_area t_cfg_change p_major
  pid: 1599 ruid: 0 euid: 0 pgid: 1599 logid: 100 cmd: 'AdminConsole'
  domain: CARW edomain: CARW hostname: electra.example.net
  event: config modify user_name: a config_area: settings
  config_item: fips information: Changed FIPS: enabled=1
  ```
- If there were problems that prevented the cryptographic module from enabling FIPS 140-2 processing, they will also be audited.

4 Update and verify configurations

Contents

Replace critical security parameters

Verify allowed cryptographic services

Verify approved cryptographic algorithms and key lengths

Verify SSH client and server configurations

Restrict administrator access

Verify SNMP version 3 configurations

Replace critical security parameters

You must replace critical security parameters (CSP): firewall certificates and private keys for several services must be regenerated and each administrator password must be changed.

To comply with FIPS 140-2 requirements, these certificates, keys, and passwords must be created *after* FIPS 140-2 processing is enabled.

Table 4-1 below shows the service, the associated CSP, the required change, and the actions needed to make the change.

Table 4-1 Critical security parameter (CSP) replacement

Service	CSP	Action to take
• Admin Console (TLS) • HTTPS decryption (TLS) • Control Center (TLS) • Firewall cluster management (TLS) • Audit log signing • IPsec/IKE certificate authentication • CAC authentication • Firewall Reporter • Profiler Communication	Firewall certificate/private key	**1** Generate or import a new firewall certificate and private key. **a** Select **Maintenance | Certificate Management** and click the **Firewall Certificates** tab. **b** Click **New** to add a certificate or click **Import** to import an existing certificate and its related private key file. **2** Replace the certificate used by each service with the new firewall certificate/private key. See "Replacing certificates" on page 14 for instructions for each service. **3** Delete the old certificate and private key. **a** Select **Maintenance | Certificate Management** and click the **Firewall Certificates**. **b** Select the old certificate and click **Delete**.
TrustedSource (TLS)	Firewall certificate/private key	**1** Delete the old certificate and private key. **a** Select **Maintenance | Certificate Management** and click the **Firewall Certificates** tab. **b** In the Certificates list, select **TS_Cert_*** and then click **Delete**. **2** Re-activate the firewall license. **a** Select **Maintenance | License** and click the **Firewall** tab. **b** Click **Activate firewall** and then click **Yes**.
IKE	IKE preshared keys	Find and replace IKE preshared keys. **1** Select **Network | VPN Configuration | VPN Definitions**. **2** Modify VPN definitions with a Remote Authentication or Local Authentication type of **Password**: Change the password on the Remote Authentication or Local Authentication tab.

Table 4-1 Critical security parameter (CSP) replacement *(continued)*

Service	CSP	Action to take
IKE	IPsec manual keys	Find and replace IPsec manual keys. **1** Select **Network | VPN Configuration | VPN Definitions**. **2** Modify VPN definitions with a Mode type of **Manually Keyed VPN**: Regenerate the keys on the Crypto tab.
SSH server	SSH host key	Generate a new SSH server host key. **1** Select **Policy | Rule Elements | Services**. **2** Select **sshd** and then click **Modify**. **3** Click **Properties**. **4** Click **Generate New Host Key**.
Administrator passwords	Hashed administrator password	Change each administrator password. **1** Select **Maintenance | Administrator Accounts**. **2** Select an administrator and click **Modify**. **3** In the **Password** field, type a new password. Retype the password in the **Confirm Password** field.
Local Certificate Authority	Local CA private key	Delete local CAs. **1** From the command line, use the following command to query local CAs that have been created: `cf lca query` **2** Delete each listed CA by name using the following command: `cf lca delete name=`*[name]*

Replacing certificates

Perform these procedures to replace certificates for the following services:

Admin Console

1. Select **Maintenance | Certificate Management** and click the **SSL Certificates** tab.
2. Select the **cobra** proxy and click **Modify**.
3. Select the new certificate from the drop-down list and then click **OK**.

HTTPS decryption

1. Select **Policy | Application Defenses | Defenses | HTTPS**.
2. In the list of HTTPS Application Defenses, select each defense that is decrypting HTTP traffic and then select a new certificate from the **Firewall certificate** drop-down list.

Firewall cluster management

1. If you have an HA cluster, remove the firewalls from the cluster and restore them to standalone status. See the *High Availability* chapter of the *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03, for instructions.
2. Replace the certificate.
   a. Select **Maintenance | Certificate Management** and click the **SSL Certificates** tab.
   b. Select the **fwregister** proxy and click **Modify**.
   c. Select the new certificate from the drop-down list.
3. Reconfigure the HA cluster. See the *High Availability* chapter of the *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03, for instructions.

Audit log signing

1. Select **Monitor | Audit Management**.
2. From the **Sign with** drop-down list, select a new certificate.

IPsec/IKE

1. Select **Network | VPN Configuration | VPN Definitions**.
2. Modify the VPN definitions to replace the old certificate with the new certificate.

Control Center management

If the firewall is managed by Control Center, perform this procedure.

1. Unregister from Control Center.
   - a. Select **Maintenance | Control Center Registration**.
   - b. Click **Unregister from the Control Center Now**.
2. Replace the certificate.
   - a. Select **Maintenance | Certificate Management** and click the **SSL Certificates** tab.
   - b. Select the **ccmd** proxy and click **Modify**.
   - c. Select the new certificate from the drop-down list and then click **OK**.
3. Re-register the firewall with Control Center.
   - a. Select **Maintenance | Control Center Registration**.
   - b. Verify the server name and IP address, then click **Register with the Control Center Now**.

CAC Authentication

1. Select **Maintenance | Certificate Management** and click the **SSL Certificates** tab.
2. Select the **CAC** proxy and click **Modify**.
3. Select the new certificate from the drop-down list and then click **OK**.

Firewall Reporter

1. Select **Maintenance | Certificate Management** and click the **SSL Certificates** tab.
2. Select the **reporter** and click **Modify**.
3. Select the new certificate from the drop-down list and then click **OK**.

Profiler Communication

1. Select **Maintenance | Profiler** and click the **Advanced Options** tab.
2. Select the new certificate from the drop-down list and then click **OK**.

Verify allowed cryptographic services

Allowed and prohibited cryptographic services for firewalls in FIPS mode are listed below. Examine your firewall configuration and make adjustments as necessary.

Note: Do not configure FIPS 140-2-prohibited algorithms while FIPS 140-2 processing is enabled. All requests to use FIPS 140-2-prohibited algorithms will be rejected and audited.

Allowed cryptographic services

The following cryptographic services are allowed on firewalls in FIPS mode:

- Admin Console management
- Firewall license management
- Audit log signing and validation
- SSH client and server
- IPsec and IKE VPNs
- RADIUS authentication (MD5) (*Cannot be used for administrator login*)
- Microsoft NT authentication (MD5, DES, RC4) (*Cannot be used for administrator login*)
- SNMP v1 and v2c
- NTP (*cannot be used with MD5 authentication*)
- HTTPS encryption/decryption
- Firewall Reporter communication
- CAC authentication
- Cluster management (entrelayd)
- Control Center management
- Certificate and key management
- Secure Sendmail (via STARTTLS)
- Firewall package signature validation/decryption
- Safeword authentication (DES) (*Cannot be used for administrator login*)
- Geo-Location, Virus Scanning, and IPS downloads
- SNMP v3 when configured with SHA authentication and AES privacy
- RIPv2 and OSPF (*cannot be used with MD5 authentication*), other routing protocols
- TrustedSource queries
- Firewall Profiler communication

Prohibited cryptographic services

The following cryptographic services are not allowed on firewalls in FIPS mode:

- SSH proxy
- Secure DNS
- Hardware Acceleration (cavium)
- RIPv2 and OSPF with MD5 authentication
- SCEP certificate enrollment
- SmartFilter
- NTP with MD5 authentication
- SNMP v3 when configured with MD5 authentication and DES privacy

Services that use SSL/TLS

Services that use SSL/TLS must use TLSv1. SSLv2 and SSLv3 are not allowed.

To verify that a service is using the appropriate SSL settings, perform this procedure for HTTPS decryption Application Defenses:

1. Select **Policy | Application Defenses | Defenses | HTTPS**.
2. In the upper pane, select an Application Defense that is decrypting HTTP traffic.
3. In the lower pane, click **SSL settings**.
4. Verify that **TLS1** is selected. Clear the SSL check boxes.

Verify approved cryptographic algorithms and key lengths

Verify that all FIPS 140-2 cryptographic services are using only these approved algorithms:

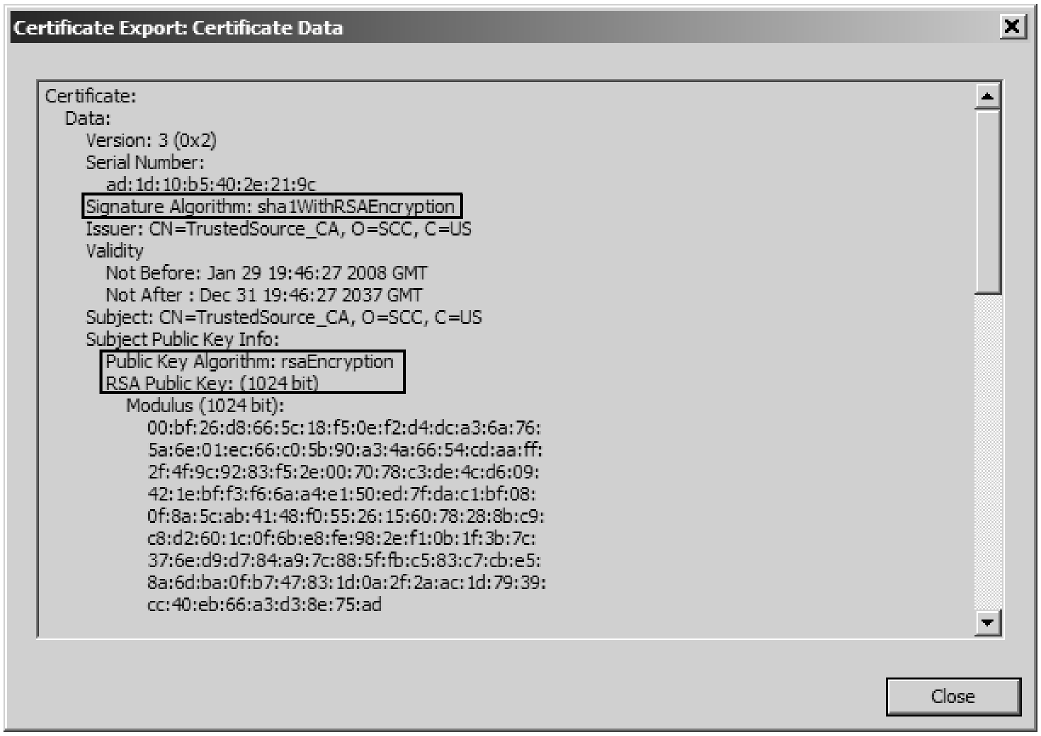
- Symmetric encryption — AES128, AES192, AES256, 3DES
- Asymmetric algorithms — RSA and DSA (minimum 1024-bit key lengths)
- Hash algorithms — SHA1, SHA2 (256, 384, 512)

- HMAC algorithms — SHA1, SHA2 (256, 384, 512)

Certificate authorities and remote certificates

Verify that certificate authorities and remote certificates are using approved cryptographic algorithms.

1. Select **Maintenance | Certificate Management**.
2. Click the appropriate tab to examine the certificates:
   - **Remote Certificates**
   - **Certificate Authorities**
3. Select the certificate you want to inspect and then click **Export**.
4. Select **Export Certificate to screen** and then click **OK**.



```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      ad:1d:10:b5:40:2e:21:9c
    Signature Algorithm: sha1WithRSAEncryption
    Issuer: CN=TrustedSource_CA, O=SCC, C=US
    Validity
      Not Before: Jan 29 19:46:27 2008 GMT
      Not After : Dec 31 19:46:27 2037 GMT
    Subject: CN=TrustedSource_CA, O=SCC, C=US
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:bf:26:d8:66:5c:18:f5:0e:f2:d4:dc:a3:6a:76:
          5a:6e:01:ec:66:c0:5b:90:a3:4a:66:54:cd:aa:ff:
          2f:4f:9c:92:83:f5:2e:00:70:78:c3:de:4c:d6:09:
          42:1e:bf:f3:f6:6a:a4:e1:50:ed:7f:da:c1:bf:08:
          0f:8a:5c:ab:41:48:f0:55:26:15:60:78:28:8b:c9:
          c8:d2:60:1c:0f:6b:e8:fe:98:2e:f1:0b:1f:3b:7c:
          37:6e:d9:d7:84:a9:7c:88:5f:fb:c5:83:c7:cb:e5:
          8a:6d:ba:0f:b7:47:83:1d:0a:2f:2a:ac:1d:79:39:
          cc:40:eb:66:a3:d3:8e:75:ad
```

Figure 4-1 Certificate Data window

5. Scroll through the certificate data to find the Signature Algorithm line. Verify that it is a FIPS 140-2-approved signature algorithm.

   If the signature algorithm is not approved, generate or import a new certificate, select the new certificate to replace the old certificate, and delete the old certificate.

IPsec and IKE

To verify that IPsec and IKE are using approved cryptographic algorithms, review VPN definition properties.

1. Select **Network | VPN Configuration | VPN Definitions**.
2. Select a VPN definition and click **Modify**.
3. Click the **Crypto** and **Advanced** tabs to review algorithms used in the definition. Modify the definition as necessary.

   Note: You might have to make corresponding adjustments to the remote peer(s).

See the *Virtual Private Networks* chapter of the *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03, for more information.

Verify SSH client and server configurations

Firewall Enterprise client and server configurations are compliant by default. If you modified either of the following configuration files, verify that your firewall's SSH client and server configuration are FIPS 140-2 compliant:

- */secureos/etc/ssh/ssh_config*
- */secureos/etc/ssh/sshd_config*

Verify the following:

- The SSH client and server are using approved cryptographic algorithms.
- SSH protocol version 1 is not allowed for the client or server. (SSH protocol version 2 is allowed.) Verify that only **Protocol 2** is enabled.
- SSH public key authentication is not allowed in FIPS mode. In the */secureos/etc/ssh/sshd_config* file, verify that **PubkeyAuthentication** is disabled.

If you have problems with SSH/SSHD, see the firewall audit for details on any FIPS-related problems. See the SSH and SSHD man pages for information about configuring SSH and SSHD.

Restrict administrator access

The following login and authentication restrictions apply to compliant firewalls:

- Administrators must use local Password authentication to log into Firewall Enterprise. All other authentication methods are prohibited for administrator login.
- Authenticated logins are required when the firewall is in Emergency Maintenance Mode. To enable authentication for Emergency Maintenance Mode, use a file editor to open */etc/ttys* and make the following change:

Locate this line:	console	none	unknown	off secure
Make this change:	console	none	unknown	off **insecure**

- You cannot log into Firewall Enterprise via Telnet. If you have a Telnet rule allowing administrator login, disable the rule.

Verify SNMP version 3 configurations

In FIPS mode, the SNMP agent will not accept version 3 requests using the FIPS 140-2-prohibited MD5 or DES cryptographic algorithms.

Add or modify an SNMP v3 user

To accept authenticated or encrypted requests, make sure the agent is configured with the FIPS 140-2-approved algorithms, SHA-1 and AES.

1. Select **Policy | Rule Elements | Services**.
2. Select **snmpd**, then click **Modify**.
3. Click **Properties**, then click **OK**.

4 In the SNMP v3 users pane:

- To add a new user, click **New**.
- To modify an existing user, select the user, then click **Modify**.

5 Select these settings:

- **Authentication type — SHA-1**
- **Privacy protocol — AES**

Tip: For additional information on adding or modifying an SNMP v3 user, refer to the *McAfee Firewall Enterprise (Sideiwnder) Administration Guide*, version 7.0.1.03, *SNMP Agent* chapter.

Verify the trap user configuration

Use this procedure to verify the trap user configuration.

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

2 Select **snmpd**, then click **Modify**.

3 Click **Properties**, then click **OK**.

4 Click the **Trap version** drop-down arrow and select **v3**.

5 Click **v3 Settings**.

6 Select:

- **Authentication type — SHA-1**
- **Privacy protocol — AES**

All attempts to send traps using MD5 or DES will fail and be audited.

Examples of audits results:

```
Jun  7 14:30:46 2010 EDT  f_snmp_agent a_fips t_error p_major
pid: 6234 ruid: 0 euid: 0 pgid: 6234 logid: 0 cmd: 'snmpd'
domain: snm3 edomain: snm3 hostname: example.host.net
event: snmp fips violation
reason: SNMP trap user is configured with authentication and privacy algorithms which
are not FIPS 140-2 compliant.
information: The SNMP trap user is configured with MD5 and DES.  See the "cf_fips" man
page or refer to the FIPS 140-2 Admin Guide for more information.


Jun  7 14:30:09 2010 EDT  f_snmp_agent a_fips t_error p_major
pid: 6231 ruid: 0 euid: 0 pgid: 6231 logid: 100 cmd: 'snmptrap'
domain: snmx edomain: snmx hostname: example.host.net
event: snmp fips violation
reason: SNMP trap user is configured with authentication and privacy algorithms which
are not FIPS 140-2 compliant.
information: The SNMP trap user is configured with MD5 and DES.  See the "cf_fips" man
page or refer to the FIPS 140-2 Admin Guide for more information.
```

5 Leave FIPS mode

If you no longer want your Firewall Enterprise to be in FIPS mode, you can re-install your firewall.

1 Enter the System Setup program and enable the CD drive in the **Boot Sequence** window.

2 Remove the tamper-evident seals and remove the bezel to gain access to the CD drive.

3 Re-install the firewall. See *Appendix B: Basic Troubleshooting* in the *McAfee Firewall Enterprise (Sidewinder) Administration Guide*, version 7.0.1.03, for instructions.

McAfee®
An Intel Company