Configuration Guide

Revision A

McAfee Firewall Enterprise 8.3.2

FIPS 140-2

The *McAfee Firewall Enterprise FIPS 140-2 Configuration Guide*, version 8.3.2, provides instructions for setting up McAfee® Firewall Enterprise (Firewall Enterprise) to comply with Federal Information Processing Standard (FIPS) 140-2.

Introduction

FIPS 140-2 is a U.S. government computer security standard used to accredit cryptographic modules.

About FIPS 140-2

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 the U.S. National Institute of Standards and Technology (NIST) and the Communications Security Establishment Canada (CSEC). Validated products that conform 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 using validated cryptographic modules and provide federal agencies with a security metric to use in procuring equipment containing validated cryptographic modules.

Firewall Enterprise models have been validated as a cryptographic module at the platform level and software levels. The McAfee Firewall Enterprise Cryptographic Module provides FIPS 140-2-compliant cryptographic services on McAfee Firewall Enterprise version 8.3.2. These services include:

- Symmetric key encryption and decryption
- Public key cryptography
- Hashing
- Random number generation

FIPS 140-2 and McAfee Firewall Enterprise platforms

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

The Firewall Enterprise hardware appliance models and software are validated to Level 2 for version 8.3.2. See the *McAfee Firewall Enterprise FIPS 140-2 Installation Guide* for your appliance model.

The Firewall Enterprise Virtual Appliance platform is validated to Level 1 for version 8.3.2.

> See the *McAfee Firewall Enterprise Control Center FIPS 140-2 Configuration Guide* for more information about configuring FIPS 140-2 on managed firewalls.

Making Firewall Enterprise FIPS 140-2 compliant

FIPS 140-2 validated mode (FIPS mode) is a separate operational state for McAfee Firewall Enterprise. Configuration changes are necessary to put your firewall in FIPS mode and make it compliant with FIPS 140-2 requirements.

This guide provides instructions to:

- Install version 8.3.2 and patch 8.3.2E14.
- Enable FIPS 140-2 processing.

See also

Install version 8.3.2 on page 2
Enable FIPS 140-2 processing on page 3
Updating and verifying configurations on page 4

Install version 8.3.2

The Firewall Enterprise installation depends on the type of firewall and the version running on the appliance.

> **Before you begin**
> To be FIPS 140-2 compliant, your Firewall Enterprise must be running version 8.3.2 and patch 8.3.2E14 when you enable FIPS 140-2 processing and update your firewall configuration.

- **Hardware appliance and software**
  - Upgrade to or install version 8.3.2

    See the *McAfee Firewall Enterprise Release Notes*, version 8.3.2, *Upgrade a firewall to version 8.3.2*.
  - Install the 8.3.2E14 patch

    See the *McAfee Firewall Enterprise Product Guide*, version 8.3.2, *Manage software packages*.
- **Virtual Appliance**
  - Upgrade to 8.3.2

    See the *McAfee Firewall Enterprise Release Notes*, version 8.3.2, *Upgrade a firewall to version 8.3.2*.
  - Install version 8.3.2

    See the *McAfee Firewall Enterprise, Virtual Appliance Installation Guide*, version 8.x.
  - Install the 8.3.2E14 patch

    See the *McAfee Firewall Enterprise Product Guide*, version 8.3.2, *Manage software packages*.

Enable FIPS 140-2 processing

Enable FIPS 140-2 processing on a Firewall Enterprise using either the Admin Console or the command line.

> The firewall must be restarted to activate the change.

> See the *McAfee Firewall Enterprise Control Center FIPS 140-2 Configuration Guide* for more information about configuring FIPS 140-2 on managed firewalls.

Tasks

- *Use the Admin Console* on page 3
  Enable FIPS 140-2 processing on a firewall using the Admin Console.
- *Use the command line* on page 3
  Enable FIPS 140-2 processing on a firewall using the command line.

Use the Admin Console

Enable FIPS 140-2 processing on a firewall using the Admin Console.

Task

1. Select **Maintenance** | **FIPS**. The FIPS checkbox appears in the right pane.
2. Select **Enable FIPS 140-2 processing**.
3. Save the configuration change.
4. A message appears stating that you must reboot Firewall Enterprise in order for changes to take effect. Click **Reboot Now**.

Use the command line

Enable FIPS 140-2 processing on a firewall using the command line.

Task

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 FIPS 140-2 setup

If FIPS 140-2 processing is successfully enabled, an audit message is generated after the firewall is restarted.

Here is an example of this audit:

```
Sept  5 16:31:42 2014 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 are problems that prevent the cryptographic module from enabling FIPS 140-2 processing, they are also audited.

Updating and verifying configurations

Replace and verify critical security parameters to ensure FIPS 140-2 compliance.

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.

The high-level steps are:

1. Create the new parameter – certificate, key, or password.
2. Select the new parameter where needed.
3. Delete the old parameter.

The following table shows the service, the associated CSP, the required change, and the actions required to make the change.

Table 1 Critical security parameter (CSP) replacement

Service	CSP	Action to take
• Admin Console (TLS) • SSL Content Inspection (TLS) • Firewall cluster management (TLS) • Audit log signing • IPsec/IKE certificate authentication • CAC authentication • CCMD • Passport authentication • Realtime Audit • McAfee® Firewall Reporter (Firewall Reporter) • McAfee® Firewall Profiler Communication • McAfee® Endpoint Intelligence Agent (McAfee EIA) (Endpoint Intelligence Agent) • Secure Alerts • SmartFilter Admin	Firewall certificate/ private key	**1** Generate or import a new firewall certificate and private key. **a** Select **Maintenance** | **Certificate/Key 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. The certificate Distinguished Name should include the full machine name. **2** Replace the certificate used by each service with the new firewall certificate and private key. See *Replace certificates* for the steps to replace the certificates. **3** Delete the old certificate and private key. **a** Select **Maintenance** | **Certificate/Key Management** | **Firewall Certificates**. **b** Select the old certificate, then click **Delete**.
Control Center (TLS)	Firewall certificate/ private key	See the *McAfee Firewall Enterprise Control Center FIPS 140-2 Configuration Guide* for more information about configuring FIPS 140-2 on managed firewalls.
Global Threat Intelligence (TLS)	Firewall certificate/ private key	**1** Delete the old certificate and private key. **a** Select **Maintenance** | **Certificate/Key Management** and click the **Firewall Certificates** tab. **b** In the **Certificates** list, select **MFE_Communication_Cert_***, then click **Delete**. **2** Reactivate the firewall license. **a** Select **Maintenance** | **License**. **b** Select a firewall from the list. **c** Select **Firewall**. **d** Click **Activate firewall**, then click **Yes**.

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

Service	CSP	Action to take
IKE	IKE preshared keys	Find and replace IKE preshared keys. 1 Select **Network | VPN Configuration | VPN Definitions**. 2 For each VPN definition, click **Modify**. The **VPN Properties** window appears. 3 Modify VPN definitions either through **Remote Authentication** or **Local Authentication**. a Select **Remote Authentication** or **Local Authentication.** b Check both tabs. If the **Method** is listed as **Password**, you must create a new one. c Enter the new password and confirm it.
IKE	IPsec manual keys	Find and replace IPsec manual keys. 1 Select **Network | VPN Configuration | VPN Definitions**. 2 For each VPN definition, click **Modify**. The **VPN Properties** window appears. 3 From the **Mode** drop-down list, look for VPN definitions that list **Manually Keyed VPN**. 4 For those with **Manually Keyed VPN**, click **Generate Keys.** New keys are generated.
SSH server	SSH host key	Generate a new SSH server host key. 1 Select **Remote Access Management | SSH Server Properties**. 2 Click **Generate new host keys**. 3 Click **Yes** to confirm. 4 Click **OK**. 5 Click **Generate new client keys**. 6 Click **Yes** to confirm. 7 Click **OK**.
Administrator passwords	Hashed administrator password	Change each administrator password. 1 Select **Maintenance | Administrator Accounts**. 2 Select an administrator, then click **Modify**. 3 In the **Password** field, type a new password. Retype the password in the **Confirm Password** field.

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

Service	CSP	Action to take

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]`

SSL CA (SSL Content Inspection)	Local CA private key	Generate a new SSL CA certificate and key. 1 Select **Maintenance** | **Certificate/Key Management** | **Certificate Authorities**. 2 Click **New** | **Single CA**. The **New Certificate Authority** window appears. 3 From the **Type** drop-down list, select **Local**. 4 Complete the fields. 5 Click **Close**. 6 Delete the old SSL CA key.
SSL server certificate key (SSL Content Inspection)	Firewall certificate/ private key	Generate a new SSL server certificate key. ℹ If you generated *SSH server* keys, you can skip the followings steps. 1 Select **Maintenance** | **Certificate** | **Key Management** | **Keys**. 2 Create new DSA and RSA keys. 3 Replace the SSL keys. a Select **Policy** | **SSL Rules**. b Examine all SSL rules. c For any that outbound, and have **Decrypt/Re-encrypt** selected, select the new DSA and RSA key. 4 Select **Maintenance** | **Cert/Key Management** | **Keys**. 5 Delete the old keys.

Replace certificates

The following table lists each service and the steps required to replace the certificate used by the service.

Table 2 Steps to replace certificates for listed services

Service	Action to take
Admin Console	1 Select **Maintenance** | **Remote Access Management** | **Admin Console Properties**. 2 From the **SSL certificate** drop-down list, select a new certificate. The certificate is replaced.
SSL Content Inspection	1 Select **Policy** | **SSL Rules**. 2 Select each rule, then click **Modify**. The **SSL Rule Properties** window appears. 3 Replace the certificate or key depending on the instance. **Scenario 1** — Type shows Inbound a If **Type** shows **Inbound** and Action shows **Decrypt only** or **Decrypt and re-encrypt**, click **SSL decryption settings (client to firewall).** b Change the **Certificate to present to clients** for **DSA** and **RSA**. **Scenario 2** — Type shows Outbound a If **Type** shows **Outbound** and **Action** shows **Decrypt and re-encrypt** , click **SSL decryption settings (client to firewall)** . b Change the **Key to use in server certificate** for both, **DSA** and **RSA**. c Change the **Local CA used to sign server cert.**
Firewall cluster management	1 If you have a High Availability cluster, remove the firewalls from the cluster and restore them to standalone status. For instructions, see the product guide. 2 Replace the certificate. a Select **Maintenance** | **Certificate/Key Management** | **SSL Certificates.** b Select the **fwregister** proxy, then click **Modify.** c From the **Certificate** drop-down list, select a new certificate, then click **OK**. The certificate is replaced. 3 Reconfigure the High Availability cluster. For instructions, see the product guide.
Audit log signing	1 Select **Monitor** | **Audit Management.** 2 If **Sign exported files** is selected, from the **Sign with** drop-down list, select a new certificate.
IPSec/IKE	1 Select **Network** | **VPN Configuration** | **VPN Definitions**. The **VPN Definitions** area appears. 2 For each VPN definition, select **Modify** | **Local Authentication.** 3 For definitions that use certificates for local authentication, on the **Certificate** drop-down list, select a new certificate. 4 Click **OK**. The certificate is replaced.

Table 2 Steps to replace certificates for listed services *(continued)*

Service	Action to take
CAC Authentication	1 Select **Policy** | **Rule Elements** | **Authenticators.** 2 If you see a CAC Authenticator, select it. 3 Click **Modify**. The **CAC Authenticator properties** window appears. 4 From the **Certificate** drop-down list, select a new certificate, then click **OK**.
CCMD	1 Select **Maintenance** | **Certificate/Key Management** | **SSL Certificates.** 2 Select the **ccmd** proxy, then click **Modify.** 3 From the **Certificate** drop-down list, select a new certificate, then click **OK**. The certificate is replaced.
Passport	1 Select **Policy** | **Rule Elements** | **Passport**. 2 On the **Advanced** tab, from the **Certificate** drop-down list, select a new certificate. The certificate is replaced.
Realtime Audit	From the command line, enter this command: `cf ssl set proxy=realtime_audit firewall_certs=<name>` Where *name* is your new firewall certificate.
Firewall Reporter	1 Select **Monitor** | **Audit Management** | **Firewall Reporter/Syslog**. 2 Select **Encrypt traffic to McAfee Firewall Reporter**. 3 From the **Certificate** drop-down list, select a new certificate, then click **OK.** The certificate is replaced.
Firewall Profiler Communication	1 Select **Maintenance** | **Profiler** | **Advanced Options.** 2 From the **Certificate** drop-down list, select a new certificate, then click **OK**. The certificate is replaced.
Endpoint Intelligence Agent	1 Select **Policy** | **Rule Elements** | **EIA**. 2 From the **Certificate** drop-down list, select a new certificate. The certificate is replaced.
Secure Alerts	From the command line, enter this command: `cf ssl set proxy=secure_alerts firewall_certs=<name>` Where *name* is your new firewall certificate.
SmartFilter Admin	1 Select **Policy** | **Application Defenses** | **SmartFilter**. 2 On the **SmartFilter Management** tab, click **Remote SmartFilter Administration Console**. 3 From the **Certificate** drop-down list, select a new certificate. The certificate is replaced.

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.

> 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.

Tasks

- *Modify the SSL rule settings* on page 11
  Services that use SSL or TLS must use TLS. SSLv2 and SSLv3 are not allowed. To make sure that a service is using the appropriate SSL settings, perform this procedure for SSL rules.

Allowed cryptographic services

These cryptographic services are allowed on firewalls in FIPS mode.

- Passive Passport (MLC)
- Control Center management
- Admin Console management
- IPsec and IKE VPNs
- Audit log signing and validation
- SSH client and server
- Firewall package signature validation and decryption
- CAC authentication
- RIPv2 and OSPF (*cannot be used with MD5 authentication*), other routing protocols
- Geo-Location, Virus Scanning, and IPS downloads
- SSL content inspection (SSL Rules)
- McAfee® Global Threat Intelligence™ queries
- Cluster management (entrelayd)
- Firewall license management
- Certificate and key management
- Secure Sendmail (via STARTTLS)
- RADIUS authentication (MD5) (*cannot be used for administrator logon*)
- Microsoft NT authentication (MD5, DES, RC4) (*cannot be used for administrator logon*)
- McAfee® Network Integrity Agent communication
- McAfee® ePolicy Orchestrator® communication
- NTP (*cannot be used with MD5 authentication*)
- SNMP v3 (AES and SHA-1)

Prohibited cryptographic services

These cryptographic services are not allowed on firewalls in FIPS mode.

- SSH proxy
- DNSSEC
- Hardware Acceleration (cavium)
- RIPv2 and OSPF with MD5 authentication
- SCEP certificate enrollment
- McAfee® SmartFilter®
- NTP with MD5 authentication

Modify the SSL rule settings

Services that use SSL or TLS must use TLS. SSLv2 and SSLv3 are not allowed. To make sure that a service is using the appropriate SSL settings, perform this procedure for SSL rules.

Task

1. Select **Policy** | **SSL Rules**.

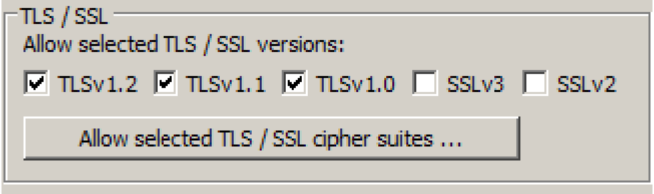
   The **SSL Rules** window appears.

2. For each rule, click **Modify**. The **SSL Rule Properties** window appears.

3. Replace the certificate or key depending on the instance.

   a. For each rule that mentions the **Action** as **Decrypt** or **Decrypt / re-encrypt**, click **SSL decryption settings (client to firewall)** and select **TLSv1**. Make sure that **SSLv2** and **SSLv3** are deselected.

   b. For each rule that mentions the **Action** as **Decrypt / re-encrypt**, click **SSL encryption settings (firewall to server)** and verify that only TLS versions are selected. Make sure that **SSLv2** and **SSLv3** are deselected.



TLS / SSL

Allow selected TLS / SSL versions:

☑ TLSv1.2 ☑ TLSv1.1 ☑ TLSv1.0 □ SSLv3 □ SSLv2

Figure 1 FIPS 140-2-compliant TLS and SSL selections

Verify approved cryptographic algorithms and key lengths

Make sure all FIPS 140-2 cryptographic services use only these approved algorithms.

- **Symmetric encryption** — AES128, AES192, AES256, 3DES
- **Asymmetric algorithms** — RSA, DSA, ECDSA (minimum 2048-bit key lengths)

  ECDSA can only be used for SSH.

- **Hash algorithms** — SHA-1, SHA-2 (256, 384, 512)
- **HMAC algorithms** — HMAC-SHA1, HMAC-SHA2 (256, 384, 512)

Tasks

- *Certificate authorities and remote certificates* on page 12

  Make sure certificate authorities and remote certificates use approved cryptographic algorithms.
- *IPsec and IKE* on page 12

  To verify that IPsec and IKE are using approved cryptographic algorithms, review VPN definition properties.
- *Passive Passport (MLC)* on page 13

  Make sure Passive Passport certificates use the RSA signature algorithm.

Certificate authorities and remote certificates

Make sure certificate authorities and remote certificates use approved cryptographic algorithms.

Task

1. Select **Maintenance | Certificate/Key Management**. The **Certificate Management** window appears.
2. Click the appropriate tab to examine the certificates:
   - **Remote Certificates**
   - **Firewall Certificates**
   - **Certificate Authorities**
3. Select the certificate you want to inspect, then click **Export**. The **Certificate Export** window appears.
4. Select **Export Certificate to screen**, then click **OK**. The **Certificate Data** window appears.
5. Scroll through the certificate data to find the **Signature Algorithm** line. Make sure that it is a FIPS 140-2-approved signature algorithm.

   If the signature algorithm is not approved, perform the following steps.

   > The minimum size of the key must be specified as 2048 bit or higher.

   a. Generate or import a new certificate.

   b. Select the new certificate to replace the old certificate.

   c. Delete the old certificate.

IPsec and IKE

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

Task

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

   > You might have to make corresponding adjustments to remote peers.

For more information, see the *VPN (virtual private networks)* chapter of the product guide.

Passive Passport (MLC)

Make sure Passive Passport certificates use the RSA signature algorithm.

Task

1 Select **Policy** | **Rule Elements** | **Passport**. The **Passport** window appears.

2 In the **Certificate** field, make sure a certificate that uses the RSA signature algorithm is specified.

3 Click **Advanced**. The **Advanced** tab appears.

4 In the **Certificate Authority** field, make sure a certificate that uses the RSA signature algorithm is specified.

Verify SSH client and server configurations

The McAfee Firewall Enterprise client and server configurations are compliant by default.

However, if you modified any of the following files, you must make sure your firewall SSH server and client is FIPS 140-2 compliant.

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

Verify the following:

- The SSH client and server use approved cryptographic algorithms.
- Only SSH Protocol 2 is enabled (SSH Protocol 1 is not allowed for the client or server).
- In the /secureos/etc/ssh/sshd_config file, PubkeyAuthentication is disabled (SSH public key authentication is not allowed in FIPS mode).

If you have problems with SSH or SSHD, view 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

These logon and authentication restrictions apply to FIPS 140-2-compliant firewalls.

- Administrators must use local Password authentication to log on to McAfee Firewall Enterprise. All other authentication methods are prohibited for administrator logon.
- Authenticated logons 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 on to McAfee Firewall Enterprise through Telnet. If you have a Telnet rule allowing administrator logon, disable the rule.

Leaving FIPS mode

If you no longer want your McAfee Firewall Enterprise to be in FIPS mode, reinstall your firewall.

For instructions, refer to one of the following documents:

- **Hardware appliance and software** — See the *McAfee Firewall Enterprise Product Guide*, version 8.3.2.
- **Virtual Appliance** — See the *McAfee Firewall Enterprise, Virtual Appliance Installation Guide*, version 8.x.