FORCEPOINT

Next Generation Firewall

How to install Forcepoint NGFW in FIPS mode

6.3

Revision C

Contents

Introduction

You can use the Forcepoint Next Generation Firewall (Forcepoint NGFW) in FIPS mode to comply with Federal Information Processing Standards (FIPS).

The Forcepoint NGFW solution includes NGFW Engines, Forcepoint NGFW Security Management Center (SMC) server components, and SMC user interface components. The basic SMC components are the Management Server, Log Server, and one or more Management Clients. The Management Client is the user interface for the SMC. You use the Management Client for all configuration and monitoring tasks.

There are two main ways to deploy the SMC:

- You can use a Forcepoint NGFW Security Management Center Appliance (SMC Appliance) that ships with a Management Server and a Log Server pre-installed on it.
- You can install the SMC on Windows or Linux platforms.

In a FIPS environment, you must use NGFW Engines that run on purpose-built Forcepoint NGFW appliances.

Installing the SMC Appliance in FIPS mode

You can install the SMC Appliance in FIPS mode.

You must complete the following main steps:

1) Enable FIPS mode on the SMC Appliance.

2) Check the self-test results on the SMC Appliance.

3) Install the Management Client in FIPS mode.

Enable FIPS mode on the SMC Appliance

You must enable FIPS mode when you install the SMC Appliance.

Steps

1) Turn on the SMC Appliance.

2) Select the keyboard layout for accessing the SMC Appliance on the command line.

3) Accept the EULA.

4) Enter the administrator account name and password.
   a) Enter the administrator account name.
      This field is case sensitive and limited to eight characters.
   b) Enter the password.
      The password is case sensitive and must have a minimum of ten characters.
   c) Enter the password again.

   Note: The administrator account and password are used for command line access to the SMC Appliance and for access to the Management Client.

5) Make your security selections.
   a) Select FIPS 140-2 mode.
   b) (Optional) Select 256-bit encryption as the security strength.

6) Select whether to configure a secondary management interface.

7) Complete the network interface and network setup fields.
   a) Select the main network interface for management.
   b) Complete the network setup fields for the interface.

8) (Secondary management interface only) Complete the network interface and network setup fields for the second network interface for management.

9) Enter a host name for the Management Server.

10) Select the time zone.

11) Set the time.

12) (Optional) Configure NTP server settings.

Result

When the installation is complete, the SMC Appliance restarts.

Check the SMC Appliance self-tests

The SMC Appliance contains several modules that run self-tests when the SMC Appliance starts.

Known answer tests (KAT) and pairwise consistency tests (PCT) are run.

Table 1: Bouncy Castle FIPS API software module self-tests

Algorithm	Type
Software Integrity	KAT
AES	KAT
CCM	KAT
AES-CMAC	KAT
FFC KAS	KAT
DRBG	KAT, Continuous, Health Checks
DSA	KAT, PCT
ECDSA	KAT, PCT
GCM/GMAC	KAT
HMAC	KAT
ECC KAS	KAT
RSA	KAT, PCT
SHS	KAT
TDES	KAT
TDES-CMAC	KAT
Extendable-Output functions (XOF)	KAT
Key Agreement Using RSA	KAT
Key Transport Using RSA	KAT
NDRNG	Continuous
DH	PCT
SP 800-56A	Assurances

Table 2: OpenSSL FIPS Object Module self-tests

Algorithm	Type
Software Integrity	KAT

Algorithm	Type
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
XTS-AES	KAT
AES CMAC	KAT
TDES	KAT
TDES CMAC	KAT
RSA	KAT, PCT
DSA	PCT
DRBG	KAT, Continuous
ECDSA	KAT, PCT
ECC CDH	KAT

Check the self-test results in the console.

- If the Bouncy Castle FIPS API cryptographic module self-test fails, the server application fails to start and an error message is shown on the console. The error message is also sent to SMC Appliance syslog.

```
Starting Forcepoint NGFW Management Server:                    [FAILED]
SMC: Cryptographic self-tests failed. Try restarting the server
Starting Forcepoint NGFW Log Server:                           [FAILED]
SMC: Cryptographic self-tests failed. Try restarting the server
```

- If a power-up self-test fails, an error message is shown on the console and the appliance turns off and is not remotely accessible.

```
fipstest: Performing FIPS RNG selftest…
Fatal FIPS Error: fipstest:ERROR:FIPS RNG selftest failed.
Failed tests: /lib/fips/fipstest-rng.sh: 1
fipstest: Performing FIPS OpenSSL crypto selftests…
Fatal FIPS Error: fipstest:ERROR:FIPS OpenSSL crypto selftest failed: /lib/fips/fipstest-ossl: 1
```

- If the file system integrity check fails, an error message is shown on the console and the appliance turns off and is not remotely accessible.

```
fipscheck: Performing FIPS integrity check…
Fatal FIPS Error: fipscheck:ERROR:FIPS check failed. /lib/fips/fipscheck: 1
```

Next steps

- If the self-tests succeed, continue configuring the SMC Appliance.
- If a self-test fails, and the SMC Appliance does not restart automatically, restart it manually.
- If a self-test continues to fail, reset the SMC Appliance to factory settings.

Reset the SMC Appliance to factory settings

If a self-test fails on the SMC Appliance, reset the SMC Appliance to factory settings.

Steps

1) Connect to the SMC Appliance command line using one of these options.
   - Connect a keyboard to a USB port and a monitor to the VGA port, then press **Enter**.
   - Connect to the IP address of the iDRAC port, then start the virtual console on the **Server Properties** tab.
2) Turn on the SMC Appliance, and at the boot menu, select **Virtual CD**.
3) Press **N** to start a new installation.
4) Press **I** to start the installation.
5) Enter `Erase`, then press **Enter** to erase the disk.
6) When prompted, press **Y** to reboot the SMC Appliance.
7) Install the SMC Appliance in FIPS Compatible Mode.

Installing the SMC

If you do not have a pre-installed SMC Appliance, you can install the SMC components in Windows and Linux environments.

For detailed installation instructions and information about hardware requirements for third-party hardware, see the *Forcepoint Next Generation Firewall Installation Guide*.

You must complete the following main steps:

1) Download the SMC software from https://support.forcepoint.com, then check the file integrity.
2) Obtain licenses for all the SMC servers and the Forcepoint NGFW Engine in the License Center at https://stonesoftlicenses.forcepoint.com.
   Generate the licenses based on your Management Server proof-of-license (POL) code.
3) Install the Management Server, the Log Server, and the Management Client, and enable FIPS restrictions on them during the installation.

Install the SMC components

To use the SMC in FIPS mode, you must enable FIPS restrictions on the Management Server, the Log Server, and the Management Client during the installation.

CAUTION: In Linux, cryptographic modules use /dev/random as the randomness source, and that may block installation, startup, or even execution. We recommend that you install and run an entropy daemon, such as jitterentropy-rngd or haveged.

Steps

1) Start the **Installation Wizard**, accept the License Agreement, then select **Typical** as the installation type.

2) Select the Management Server's IP address from the list.

3) In the **Log Server IP Address** field, enter the IP address to which this Management Server sends its log data.

4) (Optional) To use 256-bit encryption for communication between the Management Server and the NGFW Engines, select **256-bit Security Strength**.

5) Select **Enable FIPS 140-2 Configuration Restrictions**.
When the installation type is **Typical** and you enable FIPS 140-2 Configuration Restrictions on the Management Server, the restrictions are also automatically enabled on the Log Server and on the Management Client.

   Note: If you install the Log Server or the Management Client separately, you must separately enable the FIPS restrictions for them in the installation wizard.

6) Leave **Install as a Service** selected to make the Management Server start automatically.

7) (256-bit Security Strength only) Click **Next**.

8) Click **Next**.
You are prompted to create a superuser account.

   Important: This account is the only one that can log on after the installation.

9) In the **Enter the User Name** field, enter a user name.

10) In the **Enter the Password** and **Confirm the Password** fields, enter and confirm the password.

11) Click **Next**.

Next steps

Install the Log Server as described in the *Forcepoint Next Generation Firewall Installation Guide*, then install the Forcepoint NGFW Engine.

Install the Management Client in FIPS mode

If you are using the SMC Appliance or if you did not install the Management Client on the same computer as the Management Server, you must separately install the Management Client in FIPS mode.

You can use Java Web Start or download the Management Client file. For system requirements, see the SMC release notes for your version.

Note: For information about configuring the Management Server properties, see the *Forcepoint Next Generation Firewall Product Guide*.

Run the Management Client using Java Web Start

Use a web browser to distribute Management Clients from the Management Server to other computers.

Note: When you use the pre-installed SMC Appliance, Java Web Start is enabled by default on the Management Server.

Steps

1) From the client computer, connect to the Management Server using a web browser.
   `http://<IP address>:<port>`
   <IP address> is the IP address of the Management Server used for distributing the Management Clients, and *<port>* is the listening port (8080 by default). You can later change the port.

2) Click the Web Start Management Client link.

Next steps

Install the Forcepoint NGFW Engine.

Install the Management Client using a file

Download the Management Client file and install it on other computers.

Steps

1) Go to the License Center at https://stonesoftlicenses.forcepoint.com, then obtain licenses for the Management Server, the Log Server, and the NGFW Engine.

2) Go to https://support.forcepoint.com/Downloads, enter your logon credentials, then navigate to the appropriate product and version.

3) Download the Management Client .zip file.

4) Extract and run the setup.exe (Windows) or setup.sh (Linux) file to start the installation wizard.

5) Select the installation language, then accept the End-User License Agreement.

6) Select the installation folder.

7) Select the shortcut directory for starting components and maintenance tasks.

8) Select **Management Client Only** as the component to be installed.

9) Select **Restricted Cryptographic Algorithms Compatible with FIPS 140-2** as the operating mode.

10) Review the pre-installation summary, then click **Install** to start the installation.

11) Click **Done** when the installation is complete.

12) Start the Management Client, then install the licenses for the Management Server, the Log Server, and the NGFW Engine.

Next steps

Install the NGFW Engine.

Installing the NGFW Engine in FIPS mode

You can install the NGFW Engine in FIPS mode.

You must complete the following main steps:

1) Create an element for the NGFW Engine in the Management Client.

2) Enable FIPS mode in the properties of the NGFW Engine element.

3) Install the NGFW Engine in FIPS mode.

4) Check the results of the self-tests on the Forcepoint NGFW appliance.

Create an element for the NGFW Engine

Use the Management Client to create the NGFW Engine element.

These steps are the high-level tasks. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

For more details about the product and how to configure features, click **Help** or press **F1**.

1) In the Management Client, create an NGFW Engine, then define the properties in the Engine Editor.
   Follow the normal process to define the properties of an NGFW Engine, with these exceptions:
   - On the **Advanced Settings** branch, select **FIPS-Compatible Operating Mode**.
   - On the **Advanced Settings** > **Log Handling** branch, select a suitable setting for the **Log Spooling Policy** option, depending on your network environment.

2) Save the initial configuration.

   Note: Handle the configuration files securely. They include the one-time password that allows establishing trust with the Management Server.

Install the NGFW Engine in FIPS mode

Use the NGFW Initial Configuration Wizard to install the NGFW Engine in FIPS mode.

These steps are the high-level tasks. For complete installation instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.

Note: NGFW appliances come with NGFW Engine software pre-installed. Before setting the NGFW Engine to use FIPS mode, upgrade the NGFW Engine software to the version that you want to use.

Steps

1) Download the NGFW Engine software, then validate the checksums.

   Note: Save the NGFW Engine upgrade .zip file to the root directory of the USB drive or CD media.

   For information about obtaining the installation files, see the *Forcepoint Next Generation Firewall Installation Guide*.

2) Upgrade the NGFW Engine software to the version that you want to use.

   Note: If the NGFW Engine software version is earlier than 5.10, upgrade the NGFW Engine software first to 5.10.10, then to version 6.1 or higher.

   a) In the NGFW Initial Configuration Wizard, select **Firewall/VPN** as the role.

   b) Select **Upgrade**.

   c) In the **Select Source Media** dialog box, select the appropriate media type, then click **OK**.
   The software update signature is verified.

   d) (NGFW Engine versions lower than 5.10) Select **Calculate** to verify the checksum.

e) Click **OK**.
The upgrade starts.

f) (Versions 5.10 or higher) Select **Set kernel in FIPS mode after reboot**.

g) Click **OK**.

The NGFW Engine restarts and displays the upgraded version.

3) Configure the NGFW Engine with the NGFW Initial Configuration Wizard.
Follow the normal process to define the NGFW Engine properties, with these exceptions:
- Select **FIPS-Compatible Operating Mode**.

Check the NGFW Engine self-tests

The NGFW Engine contains the OpenSSL FIPS Object Module, NGFW Cryptographic Library, and NGFW Cryptographic Kernel Module. The modules run several self-tests when the Forcepoint NGFW appliance starts.

The modules perform these tests:

- Cryptographic algorithm known answer tests (KAT)
- Software integrity tests using HMAC verification
- Conditional self-tests for CTR-DRBG
- Pair-wise consistency test (PCT) on generated RSA, DSA, and ECDSA keys
- File system integrity check using the OpenSSL FIPS Object Module and HMAC

Table 3: OpenSSL FIPS Object Module self-tests

Algorithm	Type
Software Integrity	KAT
HMAC	KAT
AES	KAT
AES CCM	KAT
AES GCM	KAT
XTS-AES	KAT
AES CMAC	KAT
TDES	KAT
TDES CMAC	KAT
RSA	KAT, PCT
DSA	PCT
DRBG	KAT, Continuous
ECDSA	KAT, PCT
ECC CDH	KAT

Table 4: NGFW Cryptographic Library self-tests

Algorithm	Type
Software Integrity	KAT
AES	KAT
TDES	KAT
DSA	PCT
RSA	KAT, PCT
ECDSA	KAT, PCT
SHS	KAT
HMAC	KAT
DRBG	KAT, Continuous
Diffie-Hellman	KAT, PCT
EC Diffie-Hellman	KAT, PCT

Table 5: NGFW Cryptographic Kernel Module self-tests

Algorithm	Type
Software Integrity	KAT
AES	KAT
TDES	KAT
HMAC	KAT
SHA	KAT

Check the self-test results in the console.

- If a cryptographic self-test or the file system integrity check fails, an error message is shown on the console and the appliance is restarted automatically.

```
FIPS: OpenSSL self-tests FAILED, rebooting…
FIPS: rootfs integrity check FAILED, rebooting…
```

Next steps

- If the self-tests succeed, continue configuring the NGFW Engine.
- If the problem persists, reset the Forcepoint NGFW appliance to factory settings.

Reset the NGFW appliance to factory settings

If a cryptographic self-test or the file system integrity check fails, you must reset the appliance to factory settings.

If the appliance is otherwise functioning correctly, but you want to destroy all cryptographic keys on the NGFW appliance, you can also reset the appliance to factory settings from the Management Client. For more information, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

1) Restart the Forcepoint NGFW appliance, then select **System restore options** from the boot menu.

2) Select **Advanced data removal options**.

3) Select the number of overwrite passes.

   A larger number of overwrites is more secure, but it might take a considerable amount of time depending on the appliance storage capacity.

   - For one pass, select **1 pass overwrite**.
   - For multiple passes, select **Custom**, then enter the number of overwrite passes.

4) Install the NGFW Engine in FIPS Compatible Mode.