Forcepoint

Next Generation Firewall

6.3 or higher

Quick Start Guide

Overview

This quick start guide provides high-level instructions for setting up pre-installed Forcepoint Next Generation Firewall (Forcepoint NGFW) appliances. This information includes installation, initial configuration, post-setup tasks, and updates.

For complete details, see the *Forcepoint Next Generation Firewall Installation Guide*.

1. Check your shipment

Inspect the box the appliance was shipped in and note if it was damaged in any way.

If the appliance itself or any components delivered with the appliance show any damage, file a damage claim with the carrier who delivered the appliance or components.

2. Get product documentation

Download the documentation for this product.

Steps

1) Go to https://support.forcepoint.com/Documentation.

   You might need to log on to access the Forcepoint support website. If you do not yet have credentials, create a customer account. See https://support.forcepoint.com/CreateAccount.

2) On the **My Documentation** page, click **All Documents**.

3) Download the NGFW and Forcepoint NGFW Security Management Center (SMC) documentation for your version, including these documents.

   - *Forcepoint Next Generation Firewall Product Guide*
   - *Forcepoint Next Generation Firewall Installation Guide*
   - *Forcepoint Next Generation Firewall Release Notes*
   - *Forcepoint NGFW Security Management Center Release Notes*

   a) Browse to the **Network Security** section.

   b) Select the **Next Generation Firewall** version to display a list of documents.

   c) Select the **Security Management Center** version to display a list of documents.

4) Download the hardware guide for your appliance model.

    a) Browse to the **Network Security Appliances** section.

    b) Select the appliance type to display a list of documents.

3. Plan your configuration

Determine the number and type of NGFW Engines to install and where to place the engines on your networks.

4. Set up the NGFW appliance

Prepare the NGFW appliance for network integration.

Steps

1) Install any additional hardware components, such as interface modules.

2) For rack-mounted NGFW appliances, install the NGFW appliance in a rack.

3) Connect the NGFW appliance to your networks.

> **Note**
>
> Do not turn on the NGFW appliance.

5. Install and configure the SMC and the Management Client

Install the Security Management Center (SMC) on a Microsoft Windows or Linux server, then install the Management Client on additional computers.

For system requirements, see the *Forcepoint NGFW Security Management Center Release Notes* for your version.

Steps

1) Go to https://support.forcepoint.com, log on to your account, then select the appropriate product and version.

2) Download the SMC installation file.

3) Go to https://stonesoftlicenses.forcepoint.com, then generate and download the license files for the SMC servers.

4) To start the SMC installation, extract and run the setup.exe (Windows) or setup.sh (Linux) file.

5) Follow the on-screen instructions to perform the initial SMC configuration.

> **Note**
>
> Configuring the Web Portal Server is optional and requires an extra license.

6) Log on to the Management Client by using the shortcut icon created during the installation.

7) When prompted, accept the Security Management Center certificate, then install the SMC server licenses.

8) (Optional) Install the Management Client on additional computers.

You can also use alternative methods to access the Management Client, such as through the SMC Web Access feature or Java Web Start. For more information, see the installation guide.

> **Note**
>
> Java Web Start is only supported in SMC version 6.7 or lower.

6. Define engine elements

Use the Management Client to configure engine elements, then export the initial configuration.

> **Note**
>
> These steps describe the basic process for creating Single Firewall, Single IPS, and Single Layer 2 Firewall elements. For cluster or virtual elements, see the installation guide.

Steps

1) Go to https://stonesoftlicenses.forcepoint.com, then generate and download the license files for the engines.

> **Note**
>
> Each engine requires a separate license. If you use the Plug and Play configuration method, you do not need to create the licenses manually.

2) Select ☰ **Menu** > **System Tools** > **Install Licenses**.

3) In the dialog box that opens, select one or more license files to install, then click **Install**.

4) Add the NGFW Engine.

    a) Select ⚙ **Configuration**.

    b) Right-click **NGFW Engines**, select **New**, then select the type of engine.

c) Enter the name and Log Server information, then configure other options as needed.

5) Add two or more interfaces.

a) Select **Interfaces**, click **Add**, then select the type of interface (typically **Physical**).

b) Configure the interface properties, then click **OK**.

> **Note**
>
> Depending on the NGFW appliance model, you might need to configure additional interfaces such as wireless interfaces, modem interfaces, or an integrated switch. See the installation guide and the hardware guide for your model.

6) Add an IP address for each non-wireless interface.

> **Note**
>
> You cannot add an IP address for modem interfaces. Modem interfaces use DHCP to retrieve an IP address.

a) Right-click the interface, then select **New** > **IPv4 Address** or **New** > **IPv6 Address**.

b) Configure the IP address settings, then click **OK**.

c) Save your changes.

7) If your NGFW appliance has a wireless interface, add an IP address to the interface.

a) Right-click the wireless interface, then select **New SSID Interface**.

b) Configure the interface settings.

c) Right-click the SSID interface, then select **New** > **IPv4 Address** or **New** > **IPv6 Address**.

d) Configure the IP address settings, then click **OK**.

e) Save your changes.

8) If your NGFW appliance has an integrated switch, add an IP address to the port group interface.

a) Right-click the switch, then select **New Port Group Interface**.

b) Configure the interface settings.

c) Right-click the port group interface, then select **New** > **IPv4 Address** or **New** > **IPv6 Address**.

d) Configure the IP address settings, then click **OK**.

e) Save your changes.

9) Configure routing.

10) Save the initial configuration.

a) Select ⌂ **Home**.

b) Right-click the engine, then select **Configuration** > **Save Initial Configuration**.

c) Depending on your method, configure additional information.

■ **Automatic** — Select the time zone and keyboard layout, click **Save As** in the **USB Drive Installation** section, then save the configuration to the root directory of a USB drive.

■ **NGFW Configuration Wizard** — Make note of the one-time password, the Management Server IP address, and the Management Server certificate fingerprint. Click **View Details** to view this information.

■ **Plug and Play** — (Single Firewalls only) Select the time zone and keyboard layout, then click **Upload** in the **Installation Cloud** section.

> 📝 **Note**
>
> There are more considerations when selecting Plug and Play. For example, both the SMC and the engines must be registered for Plug and Play configuration before you configure the engines. See Knowledge Base article 9662.

d) Click **OK**.

7. Install and configure NGFW engines

Prepare the NGFW appliance, then import the initial configuration.

> 💡 **Tip**
>
> The software is pre-installed on the NGFW appliances. Do not reinstall the software unless instructed to do so by Forcepoint support.

Steps

1) Connect a computer or laptop to the NGFW appliance.

■ For Plug and Play configuration, Automatic configuration, or configuration using the NGFW Configuration Wizard on the command line, connect a serial cable to the NGFW appliance.

■ For configuration using the NGFW Configuration Wizard in a web browser, connect an Ethernet cable from the client device to physical port eth0_1 on the NGFW appliance. If the NGFW appliance does not have a port eth0_1, use port eth1_0. If using non-modular interfaces, use port eth1.

2) If you connected a serial cable to the NGFW appliance, use a terminal console program to connect to the NGFW appliance with these settings:

- **Bits per second** — 115,200
- **Data bits** — 8
- **Parity** — None
- **Stop bits** — 1.

> 📝 **Note**
>
> The serial console port speed is 115,200 bps in most NGFW appliances. The speed is 9600 bps in older NGFW appliance models. See the hardware guide for your NGFW appliance model for more information.

3) Apply the initial configuration.

Method	Task
Automatic	Insert the USB drive, then turn on the NGFW appliance. The NGFW appliance applies the initial configuration that is saved on the USB drive.
NGFW Configuration Wizard on the command line	**1)** Turn on the NGFW appliance. **2)** If you exported the initial configuration to a USB drive, start the NGFW Configuration Wizard, then insert the USB drive. > 📝 **Note** > On some NGFW appliance models, the NGFW Configuration Wizard starts automatically. For more information about the NGFW Configuration Wizard, see the installation guide. **3)** Follow the on-screen instructions to complete the configuration.
NGFW Configuration Wizard in a web browser	**1)** Turn on the NGFW appliance. **2)** On the client device, open a web browser, then connect to https://169.254.169.169. **3)** When offered a web browser client certificate, accept the certificate. **4)** Follow the on-screen instructions to complete the configuration.
Plug and Play	Turn on the NGFW appliance. The NGFW appliance connects to the Installation Server, then applies the initial configuration.

8. Upgrade the engine

Upgrade the software for a single engine to the latest version.

Steps

1) Go to https://support.forcepoint.com.

2) On the **Downloads** page, click **All Downloads**, then browse to the **Network Security** section.

3) Download the engine upgrade file, sg_engine_*version_platform*.zip.

4) Import the engine upgrade file.

    a) In the Management Client, select ☰ **Menu** > **File** > **Import** > **Import Engine Upgrades**.

    b) Select the engine upgrade file, then click **Import**.

5) Apply the upgrade.

    a) Select 🏠 **Home**.

    b) Right-click the node, then select **Upgrade Software** or **Configuration** > **Upgrade Software**.

    c) Select the operation to perform.

- **Remote Upgrade (transfer + activate)** — Installs the upgrade, then restarts the node with the new software version.
- **Remote Upgrade (transfer)** — Installs the upgrade without immediately restarting the node. The node operates with the currently installed version.
- **Remote Upgrade (activate)** — Restarts the node, then activates the new software version.

    d) Select the engine upgrade file, then click **OK**.

6) After the upgrade finishes, refresh the engine policy.

9. Perform post-setup tasks

We recommend performing these post-setup tasks; see the product guide.

Steps

1) Configure the policy and routing for the engine.

2) Set up accounts for administrators.

3) Schedule configuration backups at regular intervals.

701-0003I00