Forcepoint

NGFW Security Management Center Appliance

for Forcepoint Next Generation Firewall

Quick Start Guide

Revision C

Overview

This quick start guide provides high-level instructions for setting up a pre-installed Forcepoint NGFW Security Management Center Appliance (SMC Appliance). 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/s/article/Documentation-Featured-Article.

   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 **Tools & Links** page, click **Product Documentation**.

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 **Forcepoint Next Generation Firewall** section.

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

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

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. Prepare for installation

Prepare the SMC Appliance for network integration. For complete details, see the *Forcepoint NGFW Security Management Center Appliance Hardware Guide*.

Steps

1) Go to https://stonesoftlicenses.forcepoint.com, then generate and download the license files for the SMC servers.
2) Determine the placement and network information for the SMC Appliance.
3) Install the SMC Appliance in a rack.
4) Connect a monitor and a keyboard to the SMC Appliance.
5) Connect the SMC Appliance to your networks.

4. Complete the initial configuration

Configure the pre-installed SMC Appliance at the appliance console.

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 account name and password.
   For credential requirements, see the installation guide.
5) Make your security selections.
6) Complete the network interface and network setup fields.
7) Enter a host name for the Management Server.
8) Select the time zone.

9) Set the time.

10) (Optional) Configure NTP settings.

Result

When the installation is complete, the SMC Appliance restarts.

5. Accessing SMC Management Interface

After SMC Appliance has started, you can access the management interface in two ways:

1) Access SMC using the web access feature by navigating with a web browser to https://<IP address>:8085/.

2) Installing the management client locally and then using it connect to SMC Appliance.

For system requirements, see the SMC release notes for your version.

Note

For information about configuring the Management Server properties, see the product guide.

Access SMC using SMC Web Access

Steps

1) From the client computer, connect to the SMC Appliance using a web browser. https://<IP address>:8085.

2) Accept the warning about unknown certificate.

3) Log in with admin credentials given during installation, then import the licenses for all components.

Install the Management Client from a file

Download the SMC installer file and install it on other computers.

Steps

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

2) Download the SMC installer file appropriate for your local computer OS.

3) Extract and run the `setup.exe` (Windows) or `setup.sh` (Linux) file.

4) Select option to install Management Client component only.

5) Start the Management Client, log in with admin credentials given during installation, then import the licenses for all components.

6. Define NGFW Engine elements

Use the Management Client to configure NGFW Engine elements and export the initial configuration.

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) Add the NGFW Engine element.

2) Add two or more interfaces.

Note

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

3) Add IP addresses to the interfaces.

4) Configure the routing.

5) Save the initial configuration:
   - Save the initial configuration on a USB drive for the NGFW Configuration Wizard or the Automatic configuration method.
   - Upload the initial configuration to the Installation Server for the Plug and Play configuration method.

7. Install and configure NGFW Engines

Prepare the NGFW appliance and 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. Perform post-setup tasks

After the NGFW appliance installation and configuration is complete, use the Management Client to upload policy and manage other network elements.

Steps

1) Configure the policy and routing for the NGFW Engine.

2) Upload the policy to the NGFW Engines.

Important

Policy rules are not enforced until the policy is uploaded to the NGFW Engine.

3) Set up accounts for administrators.

4) Schedule configuration backups at regular intervals.

5) Review settings for automatic updates to keep your system current.

Published 02 February 2023

701-0067C00