

FORCEPOINT

Next Generation Firewall

**How to prepare single Forcepoint NGFW
Engines for deployment in an SD-WAN
environment**

**6.5 or higher
Revision B**

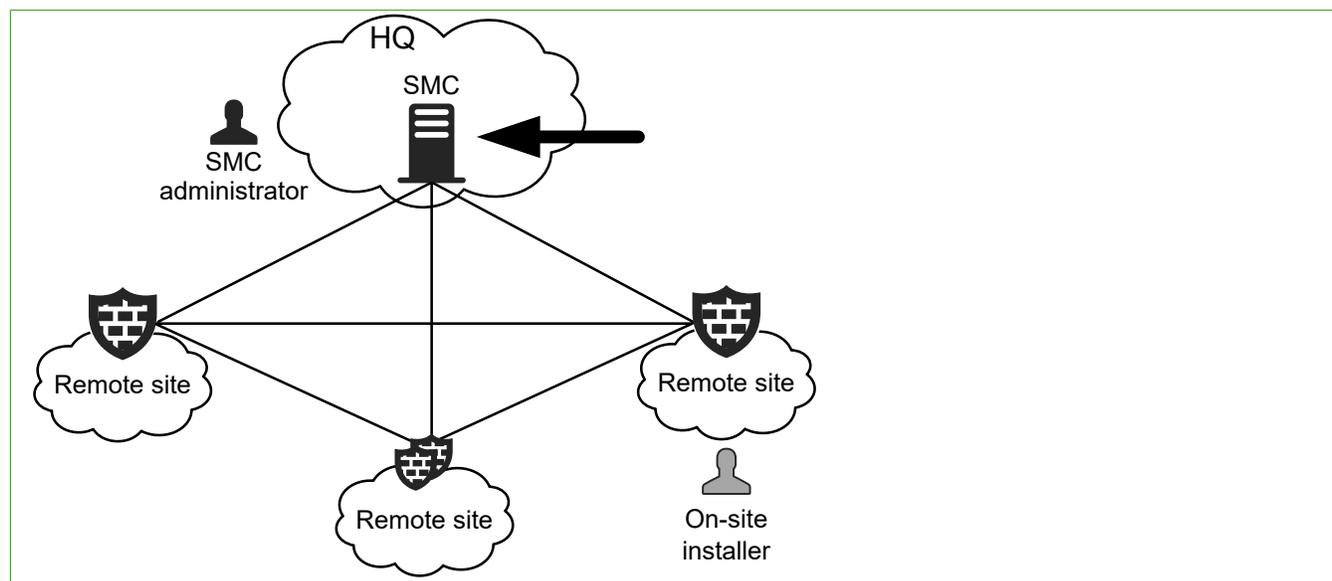
Contents

- Introduction
- Obtain licenses
- Install a license for the NGFW Engine
- Create the NGFW Engine element
- Prepare for plug-and-play configuration
- Contact the on-site installer

Introduction

This document describes the configuration steps in the Forcepoint NGFW Security Management Center (SMC) to prepare a single Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine for deployment in an SD-WAN environment.

When you deploy NGFW 51 appliances in an SD-WAN environment, pre-configured NGFW appliances are delivered to a remote site for installation using plug-and-play configuration.

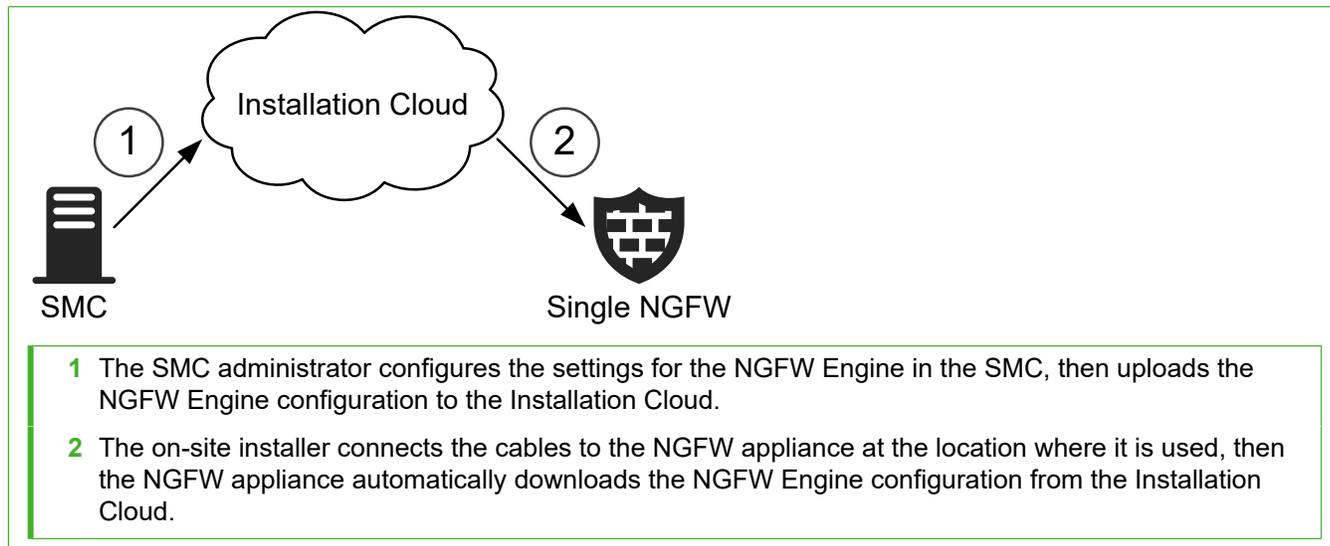


- The SMC administrator is the person who configures settings for NGFW Engines in the SMC.
- The on-site installer is the person who installs the NGFW 51 appliance at the remote site where it is used.

The tasks described in this document are to be completed by the SMC administrator. For tasks to be completed by the on-site installer, see *How to install a single NGFW appliance in an SD-WAN environment*.

Configuration overview

Configure the settings for the NGFW Engine, then upload the configuration to the Installation Cloud.



The configuration consists of the following general steps:

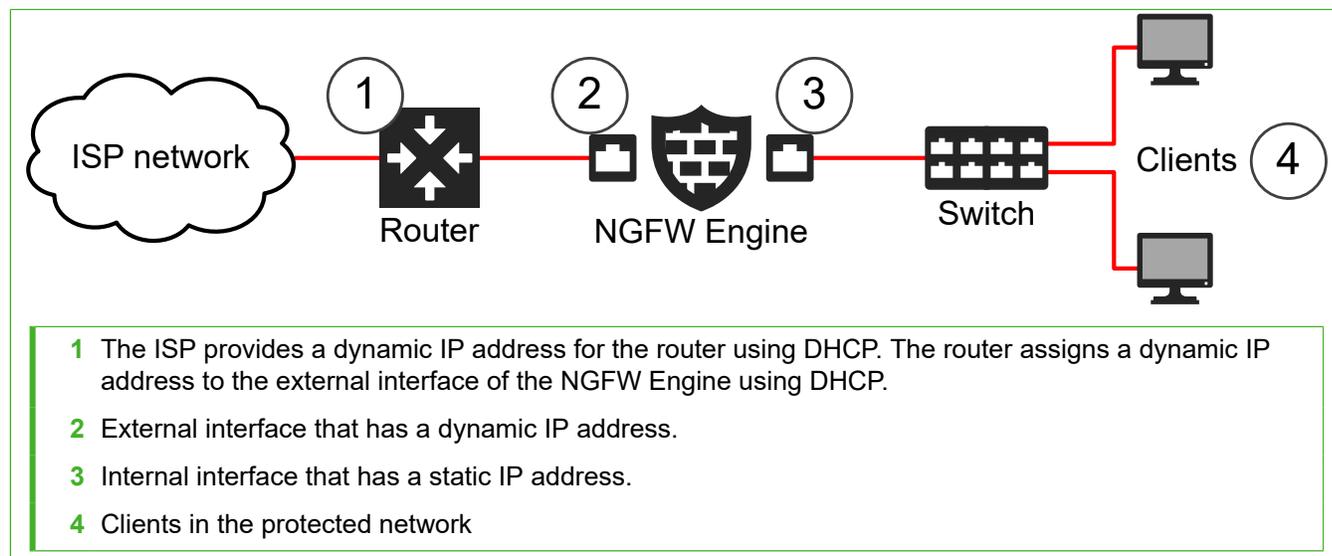
- 1) In the License Center, register the SMC and the NGFW Engine for plug-and-play configuration.
- 2) In the Management Client, install licenses for the NGFW Engine.
- 3) Create a single NGFW Engine element.
 - a) Define the interfaces.
 - b) Add the IP addresses.
 - c) Select system communication roles for the interfaces.
- 4) Save the initial configuration for the NGFW Engine, then upload it to the Installation Cloud.

When the NGFW Engine configuration is available in the Installation Cloud, the on-site installer connects the cables to the NGFW appliance at the location where it is used, and the initial configuration is automatically applied.

This document provides an overview of the configuration tasks. For more information, see the *Forcepoint Next Generation Firewall Installation Guide*.

Deployment environment

In this example deployment scenario, there is one ISP connection and a single NGFW Engine in the Firewall/VPN role at the remote site.



This deployment scenario has the following limitations:

- The LTE interface on the NGFW model 51 LTE appliance cannot be used for plug-and-play configuration. For NGFW model 51 LTE appliances, you must use Ethernet port 0 for plug-and-play configuration. After the NGFW appliance downloads and activates the configuration, you can use the LTE interface as an additional NetLink.
- The ISP connection must use DHCP to dynamically assign IP addresses. Other methods of dynamically assigning IP addresses are not supported.
- The router and the NGFW Engine must have IPv4 addresses.
- The IPS and Layer 2 Firewall roles are outside the scope of this document.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at <https://support.forcepoint.com>. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Obtain licenses

In the License Center, register the SMC and NGFW Engine for plug-and-play configuration.

Steps

- 1) Go to the License Center at <https://stonesoftlicenses.forcepoint.com>.

- 2) In the **License Identification** field, enter your SMC proof-of-license (POL) code, then click **Submit**.
- 3) Check which components are listed as included in this license, then click **Register**.
The license generation page opens.
- 4) To register the SMC and NGFW for plug-and-play configuration, click **Register your appliances for Plug & Play installation on NGFW Installation Cloud**.
- 5) Enter the NGFW appliance POS code for the appliance and your contact information, then click **Submit**.

Next steps

Install the licenses for the NGFW Engine in the Management Client.

Install a license for the NGFW Engine

Install an NGFW Engine license for the single NGFW Engine.

Before you begin

The license file must be available to the computer that you use to run the Management Client.

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

- 1) In the Management Client, select **Menu > System Tools > Install Licenses**.
- 2) Select the license file, then click **Install**.
- 3) To check that the license was installed correctly, select **Configuration**, then browse to **Administration > Licenses > All Licenses**.
One license is shown for each NGFW Engine node. POS-bound licenses are automatically bound to the NGFW Engine nodes when you install a policy on the NGFW Engine after the NGFW Engine makes initial contact with the Management Server.

Next steps

Define the single NGFW Engine elements.

Create the NGFW Engine element

Create a Single Firewall element that stores the configuration information for the NGFW Engine.

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

- 1) Select **Configuration**.
- 2) Right-click **NGFW Engines**, then select **New > Firewall > Single Firewall**.
- 3) In the **Name** field, enter a unique name.
- 4) From the **Log Server** drop-down list, select the Log Server for storing logs.
- 5) (Optional) In the **DNS IP Addresses** list, add one or more IP addresses.
- 6) (Optional) From the **Location** drop-down list, select the Location to which the NGFW Engine belongs.
- 7) Copy and paste the proof-of-serial (POS) code delivered with the appliance to the **Proof-of-Serial** field.
- 8) Click **Save**.
Do not close the Engine Editor.

Next steps

Add the interfaces.

Add layer 3 physical interfaces to the Single Firewall

Define two layer 3 physical interfaces: an external Internet-facing interface and an internal interface in the protected network.

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

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Select **Add > Layer 3 Physical Interface**.
- 3) From the **Interface ID** drop-down list, select the ID number.
 - For the external interface, select **0**.
 - For the internal interface, select **1**.

- 4) Click **OK**.
- 5) Click **Save**.
Do not close the Engine Editor.

Next steps

Add IP addresses to the layer 3 physical interfaces.

Add a dynamic IPv4 address to the external interface

Add a dynamic IPv4 address to the external Internet-facing interface.

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

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click **Interface 0**, then select **New > IPv4 Address**.
- 3) Select **Dynamic** as the type of IP address.
- 4) From the **Dynamic Index** drop-down list, select **First DHCP Interface**.
- 5) If NAT is applied between the NGFW Engine and the Management Server, add contact addresses.
 - a) If the default contact address is not dynamic, deselect **Dynamic** and enter the static contact address.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) Click **OK**.
- 7) Click **Save**.
Do not close the Engine Editor.

Next steps

Add a static IPv4 address to the internal interface.

Add a static IPv4 address to the internal interface

Add a static IPv4 address to the internal interface in the protected network.

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

- 1) In the navigation pane on the left, browse to **Interfaces**.
- 2) Right-click Interface 1, then select **New > IPv4 Address**.
- 3) In the **IPv4 Address** field, enter the IPv4 address.
- 4) In the **Netmask** field, adjust the automatically added netmask if necessary.
The Network Address and Broadcast IP address are updated accordingly.
- 5) If NAT is applied between the NGFW Engine and the Management Server, add contact addresses.
 - a) If the default contact address is not dynamic, deselect **Dynamic** and enter the static contact address.
 - b) If components from some locations must use a different IP address for contact, click **Exceptions** and define the location-specific addresses.
- 6) Click **OK**.
- 7) Click **Save**.
Do not close the Engine Editor.

Next steps

Select system communication roles for the interfaces.

Select system communication roles for Single Firewall interfaces

Select which IP addresses are used for particular roles in system communications.

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

- 1) In the navigation pane on the left, select **Interfaces > Interface Options**.

- 2) From the **Primary** control interface drop-down list, select **Interface 0**.
Because the control IP address for Management Server contact is a dynamic IP address, **Node-initiated contact to Management Server** is automatically selected.
- 3) From the **Identity for Authentication Requests** drop-down list, select **Interface 1**.
- 4) Click **Save**, then close the Engine Editor.

Next steps

Prepare for plug-and-play installation.

Prepare for plug-and-play configuration

To use plug-and-play-configuration, save the initial configuration file, then upload it to the Installation Cloud. This procedure covers the basic steps to save the initial configuration file. For complete instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.

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

- 1) In the Management Client, select **Configuration**.
- 2) Right-click the NGFW Engine for which you want to save the initial configuration, then select **Configuration > Save Initial Configuration**.
- 3) To select the policy that is automatically installed after the NGFW Engine has contacted the Management Server, click **Select**, then select the policy.
- 4) Select **Upload to Installation Server** to upload the initial configuration file automatically to the Installation Cloud.
- 5) Click **Close**.

Next steps

Contact the on-site installer.

Contact the on-site installer

After the initial configuration has been uploaded to the Installation Cloud, inform the on-site installer that the NGFW appliance is ready for installation using plug-and-play configuration.

The on-site installer installs the NGFW appliance and the initial configuration is automatically applied.

Next steps

After the on-site installer has completed the installation, check the status of the NGFW Engine in the Management Client. The configuration steps in the SMC to prepare a single NGFW Engine for deployment in an SD-WAN environment are now finished.

