

FORCEPOINT

Next Generation Firewall

**How to prepare Forcepoint NGFW Engine
clusters for deployment in an SD-WAN
environment**

6.5 or higher

Revision B

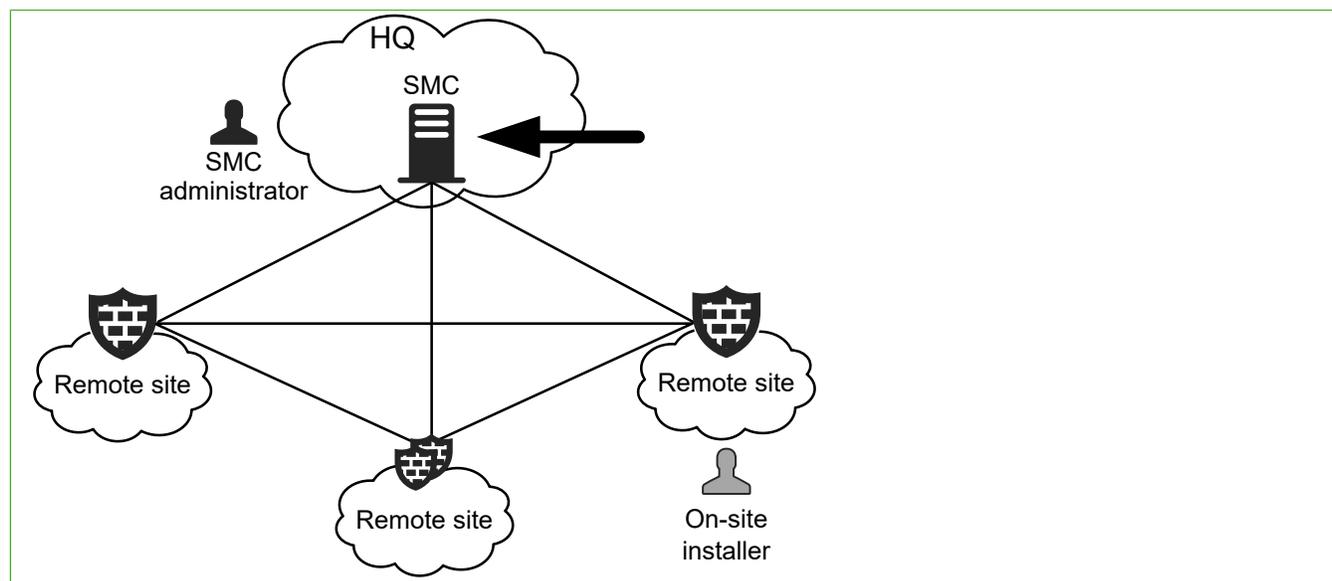
Contents

- Introduction
- Obtain licenses
- Install licenses for the NGFW Engines
- Create the NGFW Engine element
- Prepare for automatic configuration
- Provide the USB drive for automatic configuration to the on-site installer

Introduction

This document describes the configuration steps in the Forcepoint NGFW Security Management Center (SMC) to prepare a Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine cluster 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 automatic configuration.

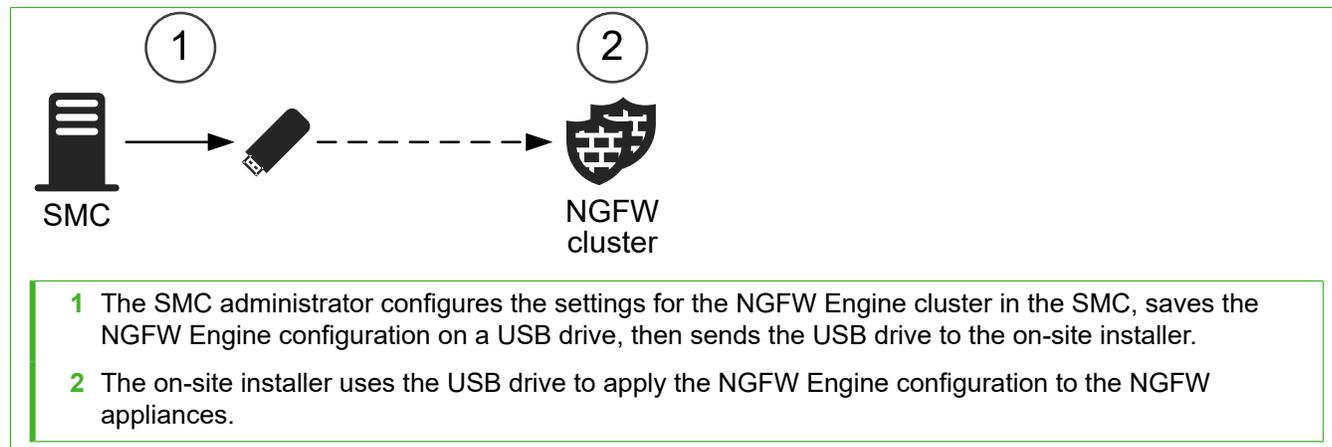


- The SMC administrator is the person who configures settings for NGFW Engines in the SMC.
- The on-site installer is the person who installs the NGFW 51 appliance at the remote site where it is used.

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 an NGFW appliance cluster in an SD-WAN environment*.

Configuration overview

Configure the settings for the NGFW Engine cluster, then save the configuration on a USB drive for automatic configuration.



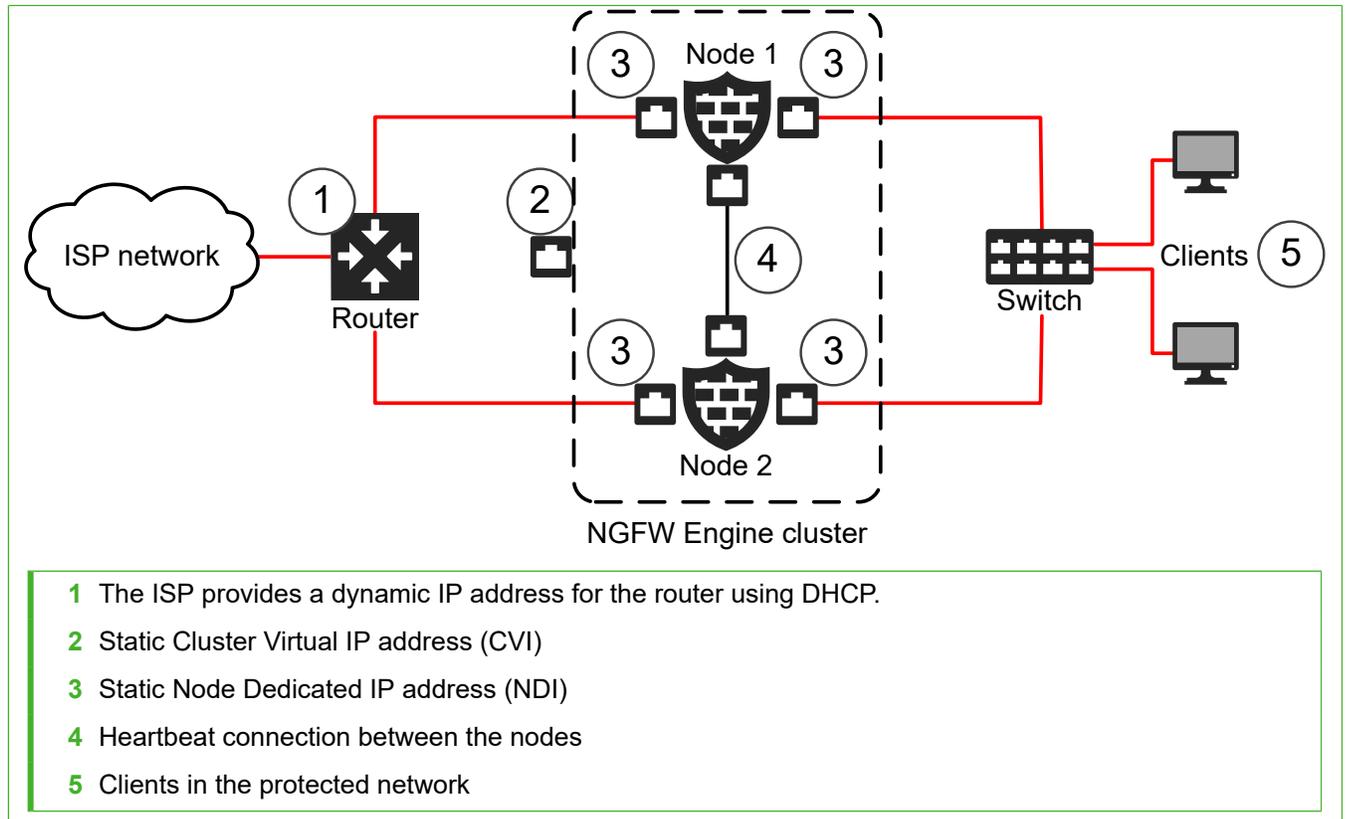
The configuration consists of the following general steps:

- 1) In the License Center, obtain licenses for the NGFW Engines.
- 2) In the Management Client, install licenses for the NGFW Engines.
- 3) Create an NGFW Engine cluster element.
 - a) Define the interfaces.
 - b) Add the IP addresses.
 - c) Select system communication roles for the interfaces.
- 4) Save the initial configuration files for the NGFW Engine cluster on a USB drive for automatic configuration.
- 5) Send the USB drive that contains the initial configuration files to the on-site installer.
- 6) The on-site installer connects the cables to the NGFW appliances and uses the USB drive to apply the initial configuration to each appliance.
- 7) When the on-site installer informs you that the NGFW appliances have been configured, refresh the policy.

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 an NGFW Engine cluster in the Firewall/VPN role at the remote site.



This deployment scenario has the following limitations:

- This deployment scenario shows an example deployment environment. The configuration and cabling might be different in your environment. Other network topologies are outside the scope of this document.
- The ISP connection must use DHCP to dynamically assign IP addresses. Other methods of dynamically assigning IP addresses are not supported.
- Although both IPv4 and IPv6 addresses are supported on NGFW Engine clusters in the Firewall/VPN role, this deployment scenario only applies to IPv4 addresses.
- This deployment scenario only applies when the NGFW Engine cluster is in the Firewall/VPN role. 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, generate licenses for the NGFW Engines.

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) Enter the Management Server's POL code or the appliance POS code for the engines you want to license.
- 5) Click **Submit Request**.
The license file is available for download on the license page.

Next steps

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

Install licenses for the NGFW Engines

Install an NGFW Engine license for each node in the NGFW Engine cluster.

Before you begin

The license files 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 files, then click **Install**.
- 3) To check that the licenses were 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 NGFW Engine cluster elements.

Create the NGFW Engine element

Create a Firewall Cluster 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 > Firewall Cluster**.
- 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) Click **Save**.
Do not close the Engine Editor.

Next steps

Add the interfaces.

Add layer 3 physical interfaces to the Firewall Cluster

Define three layer 3 physical interfaces: an external Internet-facing interface, an internal interface in the protected network, and a heartbeat 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) 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**.
 - For the heartbeat interface, select **2**.
- 4) Leave **Packet Dispatch** selected as the CVI Mode, then enter a MAC Address with an even number as the first octet.



Important: This MAC address must not belong to any actual network card on any of the nodes.

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

Add IPv4 addresses to Firewall Cluster interfaces

Add IPv4 addresses to the Firewall Cluster interfaces.

Types of IP addresses to add to each interface

Interface	Purpose	Types of IP addresses
Interface 0	External interface	CVI and NDI
Interface 1	Internal interface	NDI
Interface 2	Heartbeat interface	NDI

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**.
- 2) Configure the IP addresses for Interface 0.
 - a) Right-click **Interface 0**, then select **New > IPv4 Address**.
 - b) In the **Cluster Virtual IP Address** section, enter the IP address.
 - c) In the **IPv4 Address** field for each node in the **Node Dedicated IP Address** table, enter the IP address of each node.
 - d) If NAT is applied between the NGFW Engine and the Management Server, add contact addresses to each NDI.
 - e) Click **OK**.

- 3) Configure the IP addresses for Interface 1 and Interface 2.
 - a) Right-click **Interface 1** or **Interface 2**, then select **New > IPv4 Address**.
 - b) Deselect **Cluster Virtual IP Address**.
 - c) In the **IPv4 Address** field for each node in the **Node Dedicated IP Address** table, enter the IP address of each node.
 - d) If NAT is applied between the NGFW Engine and the Management Server, add contact addresses to each NDI.
 - e) Click **OK**.
- 4) Click **Save**.
Do not close the Engine Editor.

Select system communication roles for Firewall Cluster 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**.
- 3) From the **Primary** heartbeat interface drop-down list, select **Interface 2**.
- 4) From the **Identity for Authentication Requests** drop-down list, select **Interface 0**.
- 5) Click **Save**.

Next steps

Prepare for automatic configuration.

Prepare for automatic configuration

To use automatic configuration, save the initial configuration on a USB drive.

The initial configuration files for the NGFW Engine cluster include information for both nodes. The on-site installer can use the same USB drive to configure both nodes.

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 cluster, then select **Configuration > Save Initial Configuration**.
- 3) To select the policy that is automatically installed on the engine after the engine has contacted the Management Server, click **Select**, then select the policy.
- 4) Click **Save As**, then save the configuration files to the root directory of a USB drive. Do not change the default file name.
- 5) Click **Close**.

Next steps

Provide the USB drive to the on-site installer.

Provide the USB drive for automatic configuration to the on-site installer

After you have saved the initial configuration on a USB drive, provide the USB drive to the on-site installer.

Steps

- 1) Send the USB drive that contains the initial configuration for the NGFW Engine cluster to the on-site installer.



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

- 2) When the on-site installer informs you that both NGFW appliances have been successfully configured, refresh the policy for the NGFW Engine cluster.

Result

The configuration steps in the SMC to prepare an NGFW Engine cluster for deployment in a SD-WAN environment are now finished.

