



NGFW Manager and VPN Broker

7.2.1

Product Guide

© 2024 Forcepoint

Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.

Published 28 March 2024

Every effort has been made to ensure the accuracy of this document. However, Forcepoint makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Forcepoint shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Contents

Preface	5
Getting started	7
1 Getting started with the Forcepoint NGFW Manager and the VPN Broker	9
Parts of the NGFW Manager user interface.....	9
VPN Broker configuration	17
2 Configuring a single VPN Broker	19
Getting started with the VPN Broker.....	19
Single VPN Broker configuration overview.....	23
Start the NGFW Manager.....	24
Select the mode in the NGFW Manager.....	25
Configure an interface for members of the VPN Broker domain.....	26
Create elements for the VPN Broker configuration in the NGFW Manager.....	29
Export the VPN Broker Domain element to a file.....	37
Enable the VPN configuration in the NGFW Manager.....	37
Create elements for the VPN Broker configuration in the SMC.....	39
Check the status of the VPN Broker.....	45
3 Configuring VPN Broker high availability	47
Getting started with VPN Broker high availability.....	47
VPN Broker high availability configuration overview.....	51
Start the NGFW Manager.....	52
Select the mode in the NGFW Manager.....	54
Configure an interface for members of the VPN Broker domain.....	54
Create elements for the VPN Broker high availability configuration in the NGFW Manager.....	57
Export a VPN Broker Domain element to a file for high availability.....	67
Enable the VPN configuration in each NGFW Manager.....	68
Create elements for the VPN Broker high availability configuration in the SMC.....	70
Check the status of the VPN Broker.....	76
Local management of a single NGFW Engine	79
4 Setting up the NGFW Engine for local management	81
Example deployment scenario for a single NGFW Engine.....	81
Limitations of local management of single NGFW Engines.....	82
NGFW Engine configuration overview.....	82
Start the NGFW Manager.....	83
Select the mode in the NGFW Manager.....	84
Create elements to use for NGFW Engine configuration.....	85
Configure interfaces for connections to other networks.....	86
Edit the Access policy.....	90
Edit the NAT policy.....	94

Select the Inspection policy for the NGFW Engine.....	96
Configure SSH access to the NGFW Engine command line.....	96
Configure NTP.....	97
Configure DNS.....	98
Change the IP address of the interface for control connections.....	99
Create other elements for NGFW Engine configuration.....	100
5 Monitoring the NGFW Engine.....	103
Browse log data.....	103
Using the NGFW Engine tester.....	104
6 Configuring other NGFW Engine properties.....	109
Configure general settings for the NGFW Engine.....	109
Configure policy settings for the NGFW Engine.....	111
Configure VPN settings for the NGFW Engine.....	113
Configure log handling settings for the NGFW Engine.....	114
Add-ons for the NGFW Engine.....	115
Maintenance.....	117
7 Maintenance tasks.....	119
Upload, import, and activate dynamic update packages.....	119
Upgrade a single NGFW Engine.....	120
Change your password.....	122
Export elements.....	122
Import elements.....	123
Back up system configurations.....	123
Restore backups.....	124
Restart the NGFW Engine.....	125
Turn off the NGFW Engine.....	125
Collect information for Forcepoint support.....	126
Reset the NGFW appliance to default settings.....	126

Preface

This guide provides the information you need to work with your Forcepoint product.

Find product documentation

In the Forcepoint Customer Hub, 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 in the Forcepoint Customer Hub at <https://support.forcepoint.com>. There, you can access product documentation, release notes, Knowledge Base articles, downloads, cases, and contact information.

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





Links to downloads

NGFW Engine upgrades and dynamic update packages are available at these websites.

- NGFW Engine upgrade downloads: <https://support.forcepoint.com/Downloads>
- Dynamic update package downloads: <https://https://dep-downloads.ngfw.forcepoint.com>

Conventions

The following typographical conventions and icons are used.

<i>Book title, term, emphasis</i>	Title of a book, chapter, or topic; a new term; emphasis.
Bold	Text that is strongly emphasized.
User input, code, message	Commands and other text that the user types; a code sample; a displayed message.
Interface text	Words from the product interface like options, menus, buttons, and dialog boxes.
Hypertext	A link to a topic or to an external website.
	Note: Additional information, like an alternate method of accessing an option.
	Tip: Suggestions and recommendations.
	Important/Warning: Valuable advice to protect your computer system, software installation, network, business, or data.
	Warning: Critical advice to prevent bodily harm when using a hardware product.

Part I

Getting started

Contents

- Getting started with the Forcepoint NGFW Manager and the VPN Broker on page 9

You can use the Forcepoint NGFW Manager to configure the VPN Broker or to manage a single Forcepoint Next Generation Firewall (Forcepoint NGFW) Engine.

Chapter 1

Getting started with the Forcepoint NGFW Manager and the VPN Broker

Contents

- [Parts of the NGFW Manager user interface on page 9](#)

The Forcepoint NGFW Manager is the user interface for configuring the VPN Broker. The VPN Broker automatically creates and removes VPN tunnels as needed in full-mesh VPN environments.



Note

This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

You can alternatively use the Forcepoint NGFW Manager to locally manage a single NGFW Engine.

There are two different modes in the NGFW Manager:

- **VPN Broker Management** — Allows you to configure the VPN Broker. In this mode, elements and options related to the VPN Broker are shown in addition to elements and options related to the management of the NGFW Engine.
- **NGFW Engine Management** — Allows you to locally manage a single NGFW Engine. In this mode, elements and options related to the VPN Broker are not shown.

Before you begin configuring the VPN Broker or a single NGFW Engine, we recommend that you familiarize yourself with the NGFW Manager user interface.

Related concepts

[Getting started with the VPN Broker on page 19](#)

[Getting started with VPN Broker high availability on page 47](#)

Related information

[Setting up the NGFW Engine for local management on page 81](#)

Parts of the NGFW Manager user interface

Familiarize yourself with the parts of the NGFW Manager user interface.

The NGFW Manager consists of three main views:

- NGFW — Allows you to configure and monitor the NGFW Engine.
- SD-WAN — Shows elements used for configuring the VPN Broker, and for configuring inbound and outbound traffic management.
- Elements — Shows all elements that you can use for configuring the VPN Broker and for local management of a single NGFW Engine.

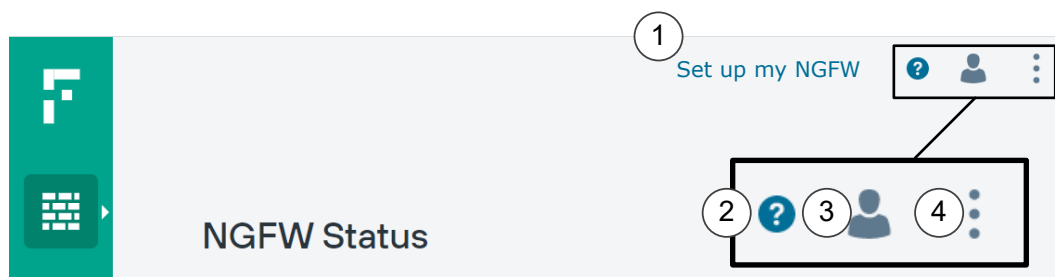


Note

This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

Controls in the NGFW Manager user interface

These general controls are available in both VPN Broker Management mode and NGFW Engine Management mode in all parts of the NGFW Manager user interface.



- 1 If you have not yet finished configuring the NGFW Engine, the **Set up my NGFW** wizard guides you through the configuration steps. After you have finished the configuration, the **Publish Changes** button is shown here.
- 2 Opens the online help in a new tab.
- 3 User actions.
 - **Log Out** — Logs you out of the NGFW Manager.
 - **Change Password** — Allows you to change your password.
 - **Mode** — Allows you to select the mode in which to use the NGFW Manager. Modes in the NGFW Manager allow you to either configure the VPN Broker or locally manage a single NGFW Engine.
- 4 Maintenance actions.

NGFW view

The NGFW view allows you to configure and monitor the NGFW Engine.

The NGFW view consists of the following tabs:

- The **Status** tab shows the status of the NGFW Engine and allows you to control the operation of the NGFW Engine.
- The **Properties** tab allows you to edit the properties of the NGFW Engine.
- The **Interfaces** tab allows you to view and edit the interface configuration of the NGFW Engine.
- The **Policy** tab allows you to view and edit the Access policy and the NAT policy.

- The **Logs** tab allows you to view log and alert entries.

NGFW > Status tab

The **Status** tab shows the status of the NGFW Engine and allows you to control the operation of the NGFW Engine.

The screenshot shows the NGFW Status tab interface. At the top right, there is a 'Publish Changes' button and user icons. The main content area is titled 'NGFW Status' and is divided into three numbered sections:

- System Information**: This section displays various system details:
 - Hostname**: Forcepoint-NGFW
 - Model**: virtual_appliance
 - Installed Policy**: Initial Policy
 - Update Package**: LLM Dynup 1322, with a 'Manage...' link.
 - Version**: 6.10.0.26010, with an 'Upgrade...' link.
 - System Time**: 3/14/2021, 11:53:11 AM
 - Up Time**: 05:20:00:23
- Getting Started**: This section provides links to help resources:
 - Online help
 - Getting started with the VPN Broker
 - Getting started with VPN Broker high availability
 - Setting up the NGFW Engine for local management
- Commands**: This section lists actions for controlling the NGFW Engine:
 - Turn Off Appliance
 - Restart Appliance
 - Reset to Default Settings
 - Information for Support

- 1** Shows information about the NGFW Engine
Allows you to manage dynamic update packages and upgrade the NGFW Engine.
- 2** Links to pages in the online Help that help you get started with the Forcepoint NGFW Manager and the VPN Broker.
- 3** Commands for controlling the operation of the NGFW Engine

NGFW > Properties tab

The **Properties** tab allows you to edit the properties of the NGFW Engine.



- 1 General settings include high-level properties of the NGFW Engine, the NGFW Engine tester, and settings for NTP and DNS.
- 2 Policy settings specify which policies the NGFW Engine uses, as well as settings for element-based NAT, alias translation, and automatic rules.
- 3 VPN settings for the NGFW Engine



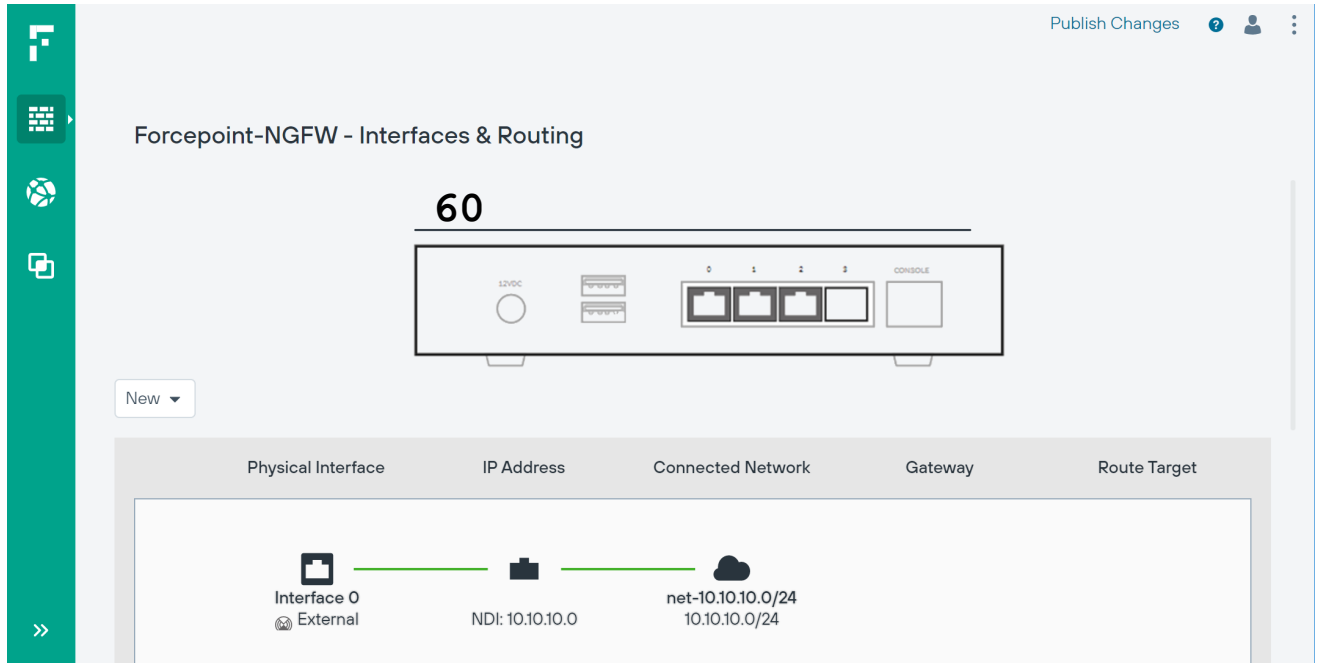
Note

VPN settings are only supported for the VPN Broker. VPN settings are not yet supported for local management of single NGFW Engines.

- 4 Log handling settings for the NGFW Engine. You can use log handling settings to configure log compression and define what happens when the log spool on the NGFW Engine becomes full.
- 5 Add-ons allow you to configure optional features for the NGFW Engine.
- 6 Other settings for the NGFW Engine

NGFW > Interfaces tab

The **Interfaces** tab allows you to view and edit the interface configuration of the NGFW Engine.

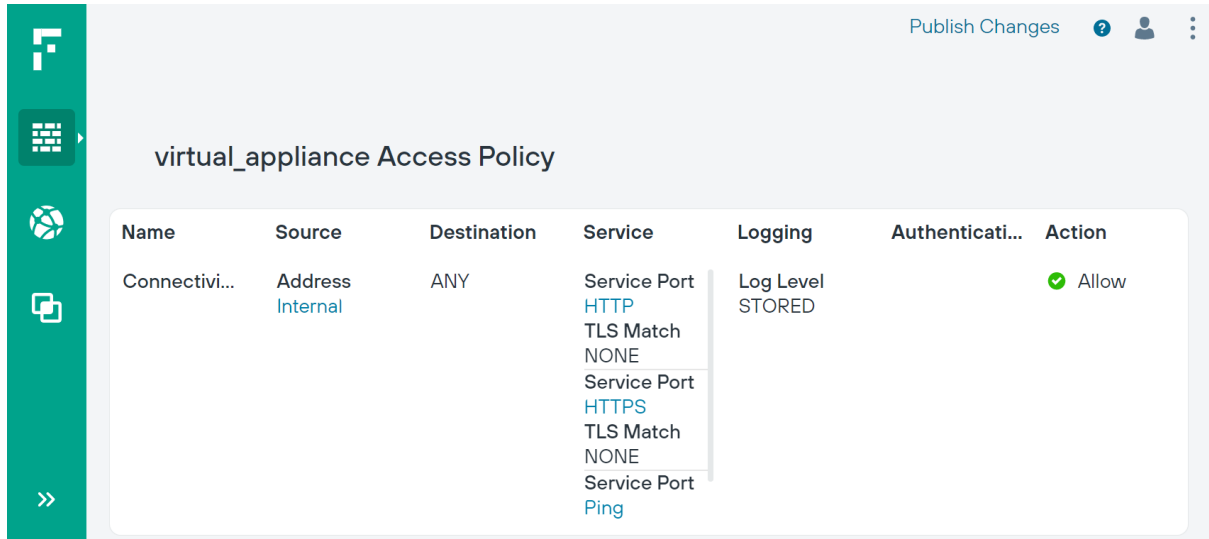


- 1 The image shows the physical ports on the NGFW appliance. When you select an interface in the interface table, the corresponding port is highlighted in the image.
- 2 Allows you to add interfaces to the interface table. Interfaces for each Ethernet port on the NGFW appliance are automatically included in the interface table.
If you change the number of Ethernet ports on the NGFW appliance, such as by replacing a 4-port interface module with an 8-port interface module, you must add interfaces to represent the new Ethernet ports.
- 3 The interface table allows you to configure the IP addresses, networks, and routing for each interface.

NGFW > Policy tab

The Policy tab allows you to view and edit the Access policy and the NAT policy.

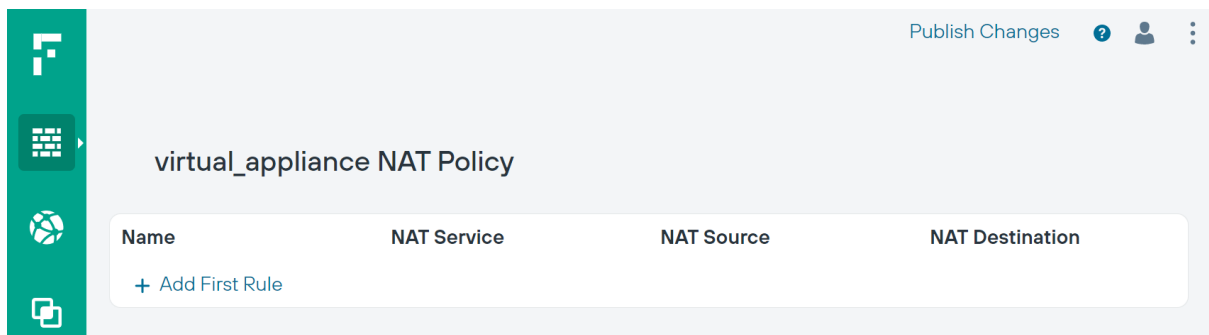
Access policy



The Access policy defines which connections the NGFW Engine allows. The rules table allows you to add and edit Access rules. By default, the NGFW Engine blocks all connections that have not been specifically allowed in the Access policy.

The Access policy also defines the logging options for traffic. Log entries are shown on the Logs tab.

NAT policy



The NAT policy defines how the NGFW Engine applies network address translation (NAT) to traffic. The rules table allows you to add and edit NAT rules.

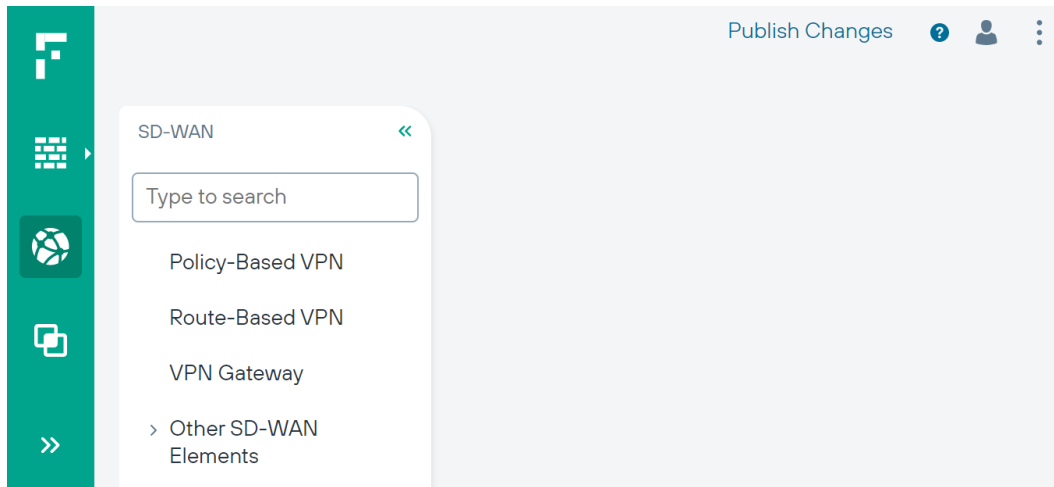
NGFW > Logs tab

The Logs tab allows you to view log and alert entries. The Logs tab shows log events in real time as they are created.

Log events																			
Kind	Creation ...	Compon...	Event ID	Sender	Informat...	Facility	Type	Action	Rule Tag	Src Addr	Dst Addr	Src Port	Dst Port	IP Protocol	IP Version	Event	Situation	Syslog	Daemon
AccessEven	2021-03-14T10:59:48.896Z	Forcepoint-NGFW node	6776819134451360804	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		
AccessEven	2021-03-14T10:59:48.900Z	Forcepoint-NGFW node	6776819134451360805	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		
AccessEven	2021-03-14T10:59:48.950Z	Forcepoint-NGFW node	6776819134451360806	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		
AccessEven	2021-03-14T10:59:49.052Z	Forcepoint-NGFW node	6776819134451360807	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		
AccessEven	2021-03-14T10:59:49.152Z	Forcepoint-NGFW node	6776819134451360808	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		
AccessEven	2021-03-14T10:59:49.352Z	Forcepoint-NGFW node	6776819134451360809	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		
AccessEven	2021-03-14T10:59:50.209Z	Forcepoint-NGFW node	6776819138746328106	169.254.169169		Packet Filtering	Notification	Discard	73292	127.0.0.1	127.0.0.1	50701	50701	17	4	Packet discarded	Connection_Discarded		

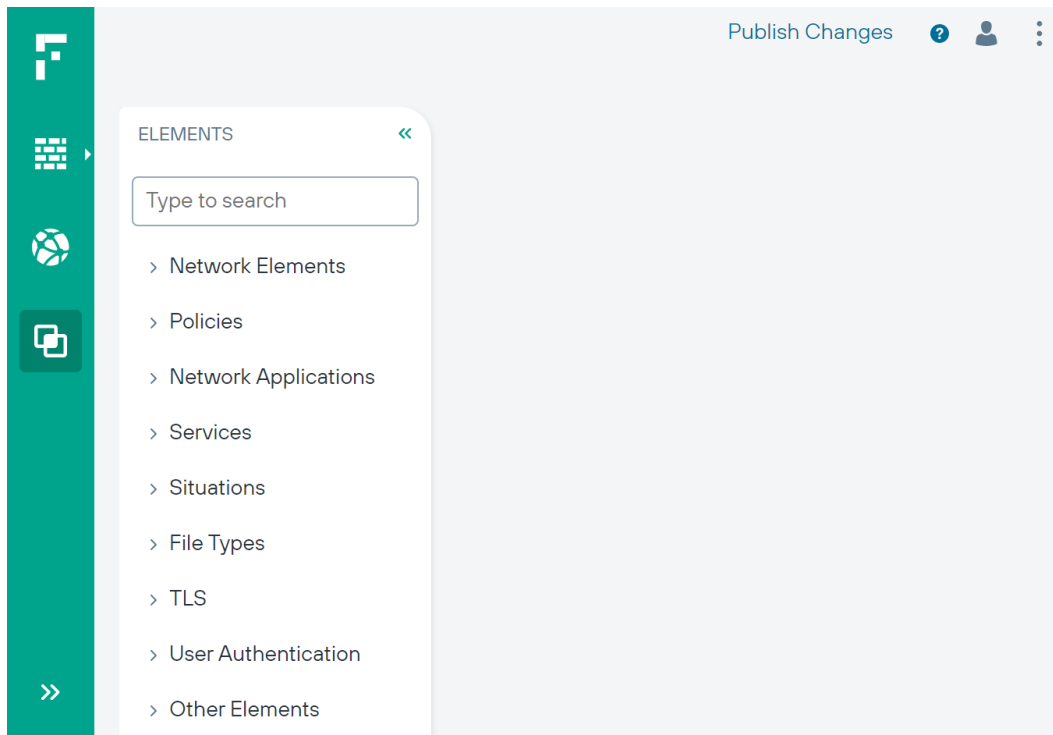
SD-WAN view

The SD-WAN view shows elements used for configuring the VPN Broker, and for configuring inbound and outbound traffic management.



Elements view

The Elements view shows all elements that you can use for configuring the VPN Broker and for local management of a single NGFW Engine.



Part II

VPN Broker configuration

Contents

- [Configuring a single VPN Broker on page 19](#)
- [Configuring VPN Broker high availability on page 47](#)

You can configure the VPN Broker as a single VPN Broker or as part of a high availability VPN Broker configuration.

Chapter 2

Configuring a single VPN Broker

Contents

- Getting started with the VPN Broker on page 19
- Single VPN Broker configuration overview on page 23
- Start the NGFW Manager on page 24
- Select the mode in the NGFW Manager on page 25
- Configure an interface for members of the VPN Broker domain on page 26
- Create elements for the VPN Broker configuration in the NGFW Manager on page 29
- Export the VPN Broker Domain element to a file on page 37
- Enable the VPN configuration in the NGFW Manager on page 37
- Create elements for the VPN Broker configuration in the SMC on page 39
- Check the status of the VPN Broker on page 45

The VPN Broker creates highly-scalable, full-mesh VPN environments. VPN tunnels are automatically created between NGFW Engines when they communicate with each other. The VPN tunnels are automatically removed when they are no longer needed.

You can configure the VPN Broker in the NGFW Manager on a dedicated Forcepoint NGFW appliance. The VPN Broker is a component of Forcepoint NGFW.



Note

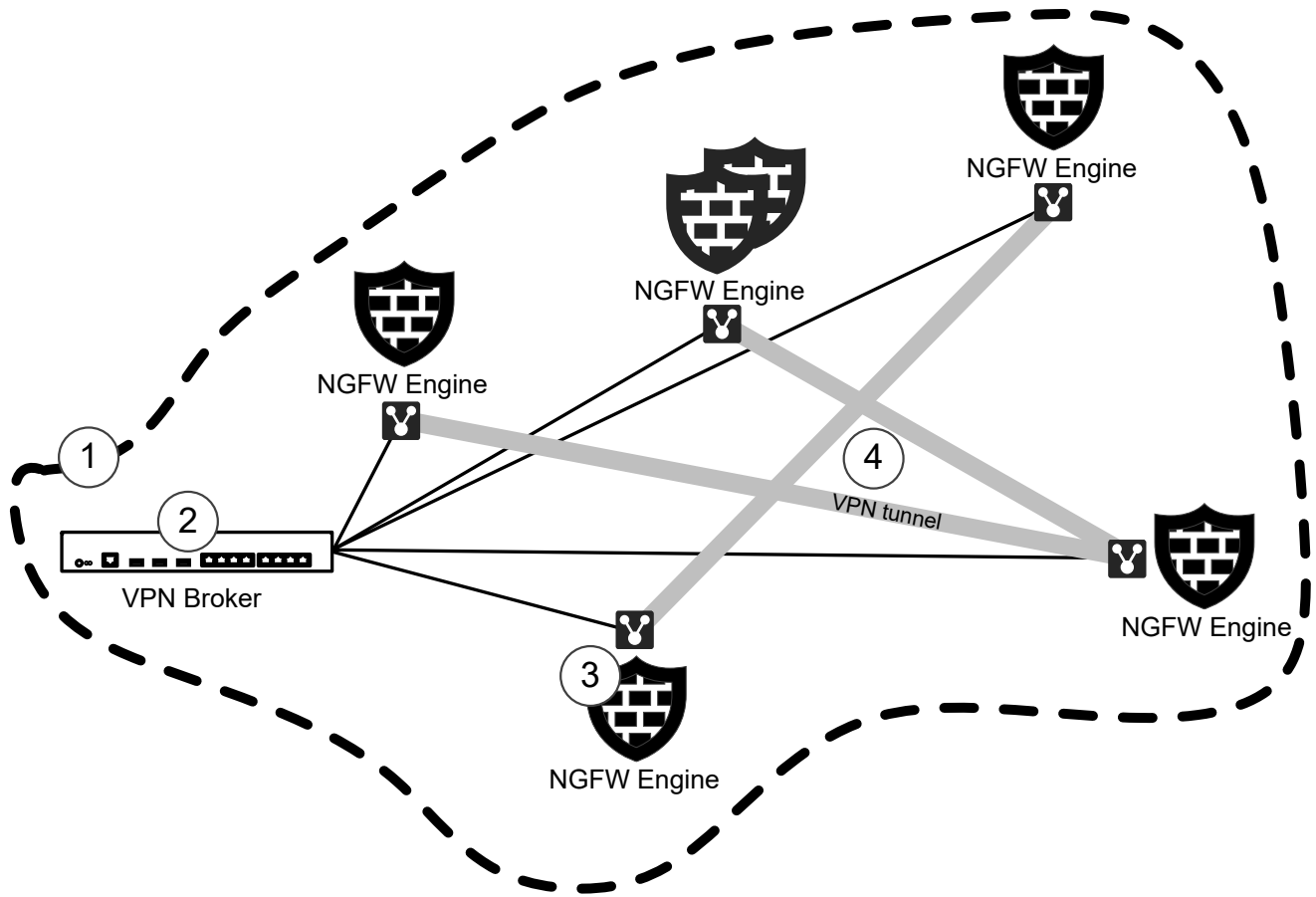
This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

Getting started with the VPN Broker

The VPN Broker environment consists of a VPN Broker domain, a VPN Broker gateway, and several VPN Broker members.

- VPN Broker domain — The VPN Broker domain is a virtual network that contains the VPN Broker gateway and the VPN Broker members.
- VPN Broker gateway — The VPN Broker gateway is configured on a single pre-installed Forcepoint NGFW appliance that is dedicated for use only with the VPN Broker.
- VPN Broker member — Each VPN Broker member is an NGFW Engine in the Firewall/VPN role (Single Firewall or Firewall Cluster). When you use Master NGFW Engines and Virtual NGFW Engines, the same Master NGFW Engine can host VPN Broker members that belong to more than one VPN Broker domain. VPN tunnels can be created between VPN Broker members that are controlled by different Management Servers. The members do not need to be in the same administrative Domain in the Forcepoint NGFW Security Management Center (SMC).

The following is an example environment for a single VPN Broker configuration.



- 1 VPN Broker domain
- 2 VPN Broker gateway
All members of the domain are connected to the same VPN Broker gateway.
- 3 VPN Broker member
- 4 VPN tunnels are created and removed as needed between the VPN Broker members.

Access rules that allow communication between the VPN Broker gateway and the members are automatically created. The communication between domain members and the VPN Broker gateway is authenticated using a shared secret.

The members communicate with the VPN Broker gateway using a VPN Broker Interface that you must configure on each NGFW Engine. The traffic that goes into the VPN also passes through this interface.

How the VPN Broker Domain works

The VPN Broker domain is a virtual network that contains the VPN Broker gateway and the VPN Broker members.

Also, the VPN Broker domain uses Internet Key Exchange (IKE) and Internet Protocol Security (IPsec) to establish secure VPN communications within VPN Broker elements. The settings used are:

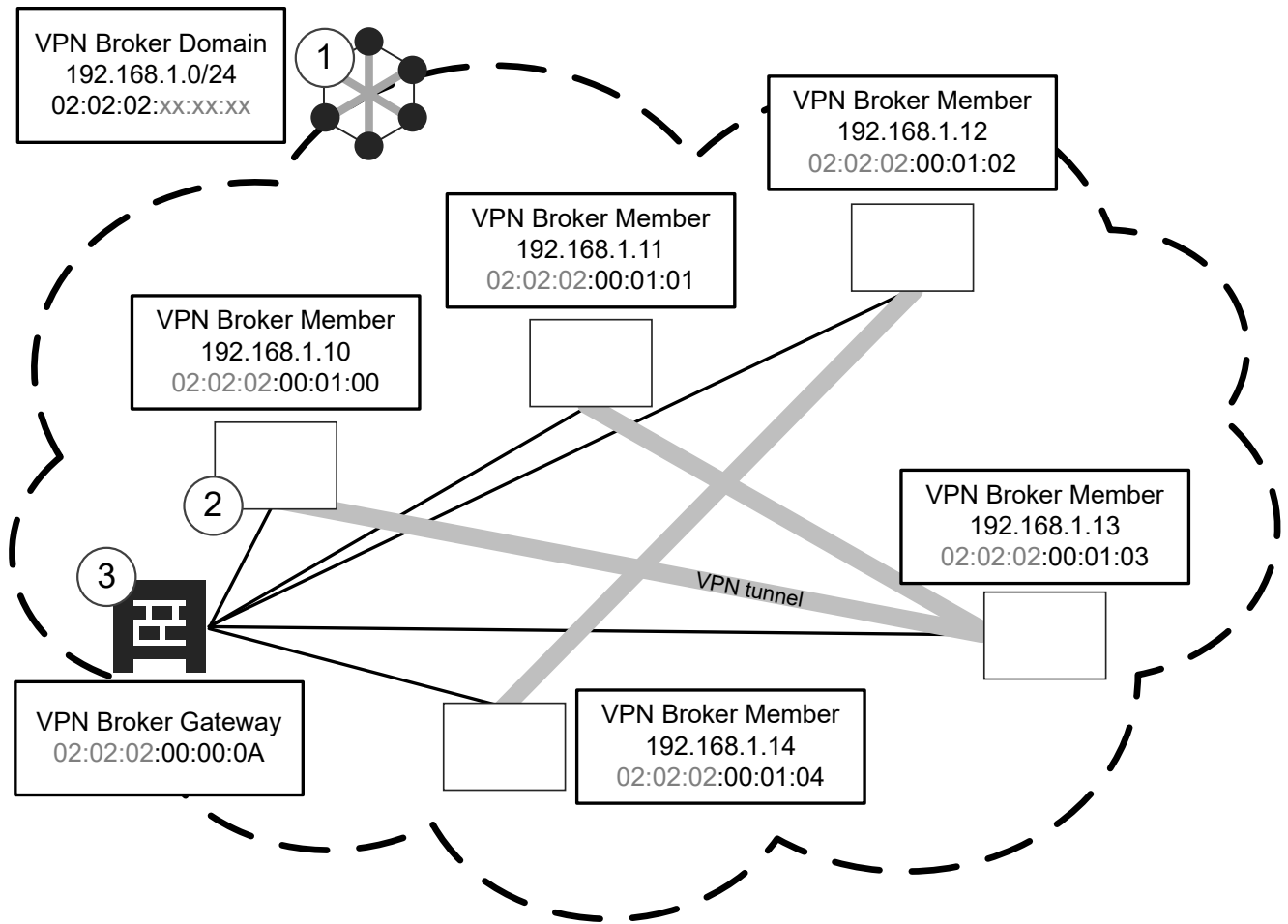
- **For IKE:**
 - Version: 2
 - Cipher: AES-256
 - Message Digest: SHA-256

- D-H Group: 15 (3072-bit MODP Group)
- Lifetime: 8 hrs
- **For IPsec:**
 - Protocol: ESP
 - Cipher: AES-GCM-256
 - Compression: None
 - D-H Group for PFS: 15 (3072-bit MODP Group)
 - Lifetime: 2 hrs

**Note**

- The settings are not user configurable.
- Authentication between VPN Broker Gateway and each VPN Broker Member is using an unique administrator specified shared secret.
- Authentication for dynamically created tunnels between VPN Broker Members is by using a 3072-bit raw RSA keys that are generated locally at each VPN Broker Member.
- VPN Broker Gateway relays public keys between members so that they can authenticate each other securely.

The following is an example of IP addresses and MAC addresses in the VPN Broker Domain.



- 1 The VPN Broker Domain is a virtual network.
The VPN Broker Domain is identified by a unique MAC address prefix. In this example, the MAC address prefix is 02:02:02.
- 2 Each VPN Broker Member has an IP address that is part of the virtual network defined in the VPN Broker Domain.
Each VPN Broker Member is identified by a unique partial MAC address.
- 3 The VPN Broker Gateway is identified by a unique VPN Broker Gateway ID number.

The MAC address prefix of the VPN Broker Domain is combined with the partial MAC address of each VPN Broker Member to form a complete MAC address for each VPN Broker Member.

Example of how VPN Broker Member MAC addresses are formed

MAC address prefix of the VPN Broker Domain	Partial MAC address of the VPN Broker Member	Complete MAC address of the VPN Broker Member
02:02:02	00:01:00	02:02:02:00:01:00
	00:01:01	02:02:02:00:01:01
	00:01:02	02:02:02:00:01:02
	00:01:03	02:02:02:00:01:03
	00:01:04	02:02:02:00:01:04

The MAC address prefix of the VPN Broker Domain is combined with the VPN Broker Gateway ID number to form a complete MAC address for the VPN Broker Gateway.

In this example, the VPN Broker Gateway ID is 10. In the NGFW Manager, you enter the VPN Broker Gateway ID as a decimal number. However, the ID is converted internally to a hexadecimal number. For example, an ID of 10 is converted to 0A in the MAC address of the VPN Broker Gateway.

Example of how VPN Broker Gateway MAC addresses are formed

MAC address prefix of the VPN Broker Domain	VPN Broker Gateway ID	Complete MAC address of the VPN Broker Gateway
02:02:02	10	02:02:02:00:00:0A

Single VPN Broker configuration overview

To configure a single VPN Broker, you must complete steps in the NGFW Manager and in the SMC.

Steps in the NGFW Manager

- 1) Start the NGFW Manager, then select VPN Broker Management mode.
- 2) Configure the interface to which members of the VPN Broker domain can connect.
- 3) Create the required elements in the following order:
 - a) VPN Broker Gateway
 - b) VPN Broker Domain
 - c) VPN Broker Member
- 4) Export the VPN Broker Domain element to a file.
- 5) Enable the VPN configuration.

Steps in the Management Client component of the SMC

- 1) Create the required elements in the following order:
 - a) Create a VPN Broker Domain element.
 - b) Add a VPN Broker Interface to the NGFW Engine.
- 2) Refresh the firewall policy.

**Note**

VPN Broker provides connectivity between networks of the VPN Broker members. You must add Access rules to the policy of each NGFW Engine to allow specific types of traffic to and from these networks.

Next steps

Begin the configuration by starting the NGFW Manager.

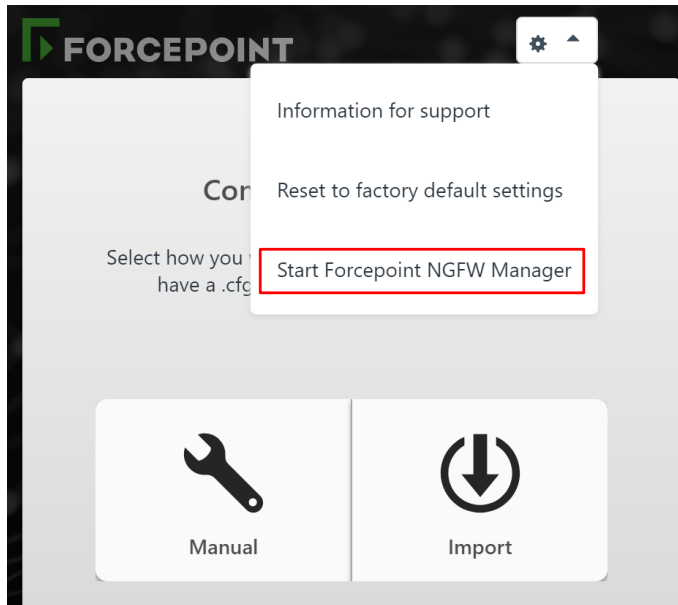
Start the NGFW Manager

The NGFW Configuration Wizard allows you to configure settings for the Forcepoint NGFW appliance. Start the NGFW Manager from the web browser version of the NGFW Configuration Wizard.

Steps

- 1) Connect the NGFW appliance to a laptop or other client device.
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) Connect the other network cables to the Forcepoint NGFW appliance.
- 3) Turn on the Forcepoint NGFW appliance.
- 4) To start the web browser version of the NGFW Configuration Wizard, open a web browser on the client device, then connect to <https://169.254.169.169>.
It might take some time for the web page to load.
- 5) When the NGFW Configuration Wizard offers a web browser client certificate, accept the certificate.
- 6) On the Welcome page of the NGFW Configuration Wizard, click **Start**.
- 7) Select **I Agree to the Terms and Conditions**, then click **Next**.

- 8) Enter and confirm the password for the root account, then click **Next**.



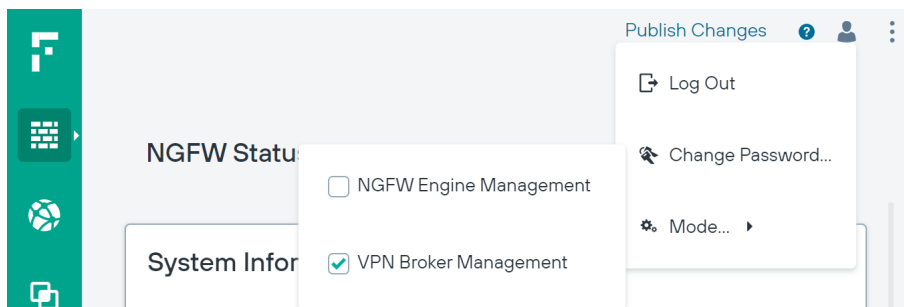
- 9) Click **⚙** > **Start Forcepoint NGFW Manager** to restart the appliance.
- 10) After the NGFW appliance has restarted, refresh the web browser to start the NGFW Manager.
- 11) Enter `root` as the user name, enter the password for the root account, then click **Log In**.

Next steps

Continue by selecting the mode in the NGFW Manager.

Select the mode in the NGFW Manager

Modes in the NGFW Manager allow you to either configure the VPN Broker or locally manage a single NGFW Engine.



Steps

- 1) Select **User** > **Mode**, then select the mode.

- **VPN Broker Management** — Allows you to configure the VPN Broker. In this mode, elements and options related to the VPN Broker are shown in addition to elements and options related to the management of the NGFW Engine.
- **NGFW Engine Management** — Allows you to locally manage a single NGFW Engine. In this mode, elements and options related to the VPN Broker are not shown.

**Note**

If you are in the **VPN Broker** branch of the **SD-WAN** view, you cannot change the mode to **NGFW Engine Management**. Browse to a different view, then change the mode.

Next steps

Continue the configuration in one of the following ways:

- If you are configuring the VPN Broker, configure an interface for members of the VPN Broker domain.
- If you are locally managing a single NGFW Engine, create elements to use for NGFW Engine configuration.

Configure an interface for members of the VPN Broker domain

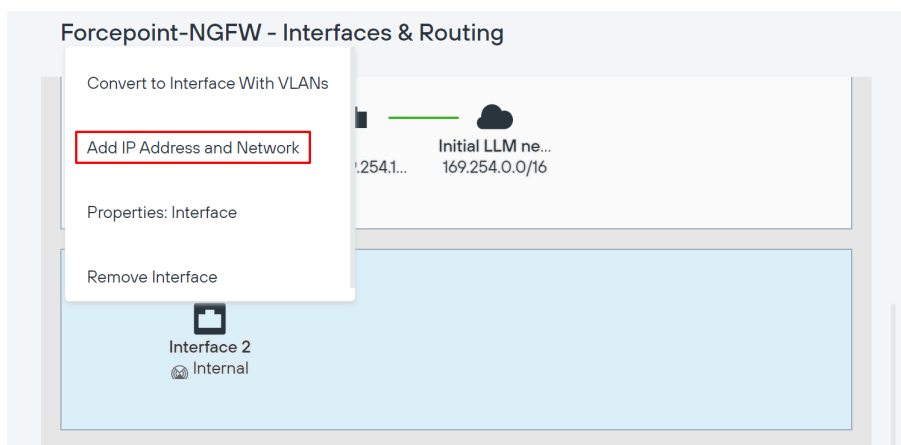
Interfaces for each Ethernet port on the NGFW appliance are automatically included in the interface table. You must add an IP address for the interface to which members of the VPN Broker domain connect.

Before you begin

Start the NGFW Manager, then select VPN Broker Management mode.

Steps

- 1) Browse to **NGFW > Interfaces**.



- 2) In the interface table below the appliance image, click an interface, then select **Add IP Address and Network**.
- 3) Enter the IP address and netmask to which members of the VPN Broker domain can connect in CIDR notation, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

Interfaces & Routing page	
Option	Definition
<div style="border: 1px solid #ccc; padding: 5px; width: fit-content; margin-bottom: 10px;">New</div>	<p>Adds an interface to the interfaces table. If you change the number of Ethernet ports on the NGFW appliance, such as by replacing a 4-port interface module with an 8-port interface module, you must add interfaces to represent the new Ethernet ports.</p> <ul style="list-style-type: none"> ■ Interface — Adds a physical interface. Opens the New Interface pane. ■ Interface with VLANs — Adds a physical interface with a placeholder for adding VLAN interfaces later. Opens the New Interface With VLANs pane. ■ Tunnel Interface — This option is not yet supported.
Appliance image	Shows the ports on the NGFW appliance for which you can configure interfaces. When you select an interface in the interface table, the corresponding port is highlighted in the image.
Interface table	Allows you to configure the IP addresses, networks, and routing for each interface.
Physical Interface	<p><i>(When interface type is Physical Interface)</i></p> <p>Shows the interface ID of the physical interfaces. The following actions are available when you click the interface:</p> <ul style="list-style-type: none"> ■ Add IP Address and Network — Adds an IP address and a Network element to the interface. Opens the New IP Address and Netmask pane. ■ Convert to Interface With VLANs — Removes any IP addresses that have been specified and converts the interface to an interface with VLANs. ■ Properties: Interface — Opens the interface properties. ■ Remove Interface — Removes the interface from the configuration.
Physical Interface	<p><i>(When interface type is Physical Interface with VLAN interfaces)</i></p> <p>Shows the interface ID of the physical interfaces and the VLAN interfaces under them. The following actions are available when you click the physical interface:</p> <ul style="list-style-type: none"> ■ Add VLAN Interface — Adds a VLAN interface. ■ Convert to Interface — Converts the interface with VLANs to an interface. There can be a maximum of one VLAN Interface when you convert the interface. ■ Properties: Interface with VLANs — Opens the interface properties. ■ Remove Interface — Removes the interface from the configuration. <p>The following actions are available when you click the VLAN interface:</p> <ul style="list-style-type: none"> ■ Add IP Address and Network — Adds an IP address and a Network element to the interface. Opens the New IP Address and Netmask pane. ■ Properties: VLAN Interface — Opens the VLAN interface properties. ■ Remove VLAN Interface — Removes the VLAN interface.

Option	Definition
IP Address	Shows the IP address of the physical interface or VLAN interface. The following actions are available when you click the IP address: <ul style="list-style-type: none"> ■ Properties: Static Address — Allows you to add a static IP address to the interface. ■ Remove IP Address and Network — Removes the IP address from the interface configuration.
Connected Network	Shows the network range of the directly connected network. The following options are available when you click the network: <ul style="list-style-type: none"> ■ Add Gateway — Allows you to add a route through a gateway device to a network that is not directly connected. ■ Properties: Network — Opens the properties of the Network element.
Gateway	Shows the gateway device through which the NGFW Engine connects to a network that is not directly connected. The following actions are available when you click the gateway: <ul style="list-style-type: none"> ■ Add Route Target — Allows you to specify the IP addresses that are reachable through the gateway device. ■ Properties: <element type> — Opens the properties of the element that represents the gateway device. ■ Remove Gateway — Removes the gateway device from the interface configuration. The element is not deleted.
Route Target	Shows the IP addresses that are reachable through the gateway device. The following options are available when you click the route target: <ul style="list-style-type: none"> ■ Properties: <element type> — Opens the properties of the element that represents the IP addresses. ■ Remove Route Target — Removes the route target from the interface configuration. The element is not deleted.

Interface properties	
Option	Definition
Interface ID	<i>(When interface type is Physical Interface)</i> The Interface ID automatically maps to a physical network port on the appliance.
VLAN ID	<i>(When interface type is VLAN Interface)</i> Specifies the VLAN ID (1–4094). The VLAN IDs must be the same as the VLAN IDs that are used in the switch at the other end of the VLAN trunk. Each VLAN Interface is identified as Interface-ID.VLAN-ID, for example, 2.100 for Interface ID 2 and VLAN ID 100.
Interface Options (Optional)	Advanced options for interface configuration.
MTU	The maximum transmission unit (MTU) size on the connected link. Enter a value between 576–65000.
Zone	The network zone to which the interface belongs. By default, Interface 0 belongs to the external zone. All other interfaces belong to the internal zone.
Log Compression Override	When selected, the log compression settings defined for the interface override the default log compression settings defined for the NGFW Engine. <ul style="list-style-type: none"> ■ Compress Discard Logs — When selected, enables log compression for discard log entries. ■ Compress Antispoofing Logs — When selected, enables log compression for antispoofing log entries.

Option	Definition
Log Rate	The maximum sustained number of log entries per second. The default value is 100 log entries per second.
Log Burst Size	The maximum number of log entries in a single burst. The default value is 1000 log entries.
Antispoofing Elements	This option is not yet supported.
Route Replies Back	This option is not yet supported.

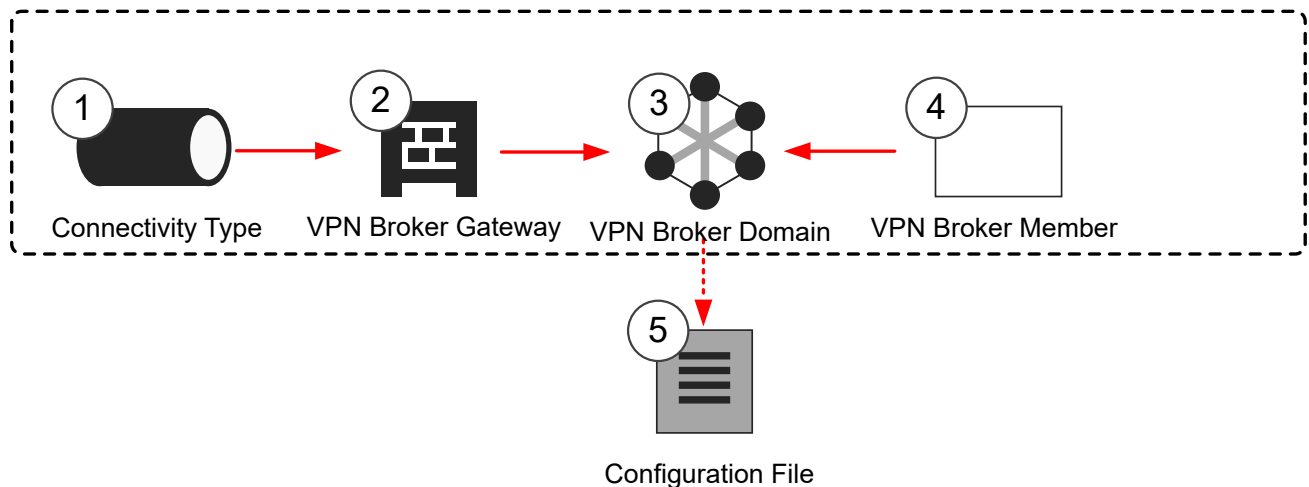
Next steps

Create elements for the VPN Broker configuration in the NGFW Manager.

Create elements for the VPN Broker configuration in the NGFW Manager

You must create the elements that represent the VPN Broker configuration in the NGFW Manager.

The following elements are used in the configuration:



- 1 Connectivity Type elements define the connectivity group to which endpoints belong, and the mode used when an endpoint is part of a Multi-Link configuration.
The default system Connectivity Type elements belong to connectivity group 1. If you need to use a different connectivity group, create a custom Connectivity Type element.
- 2 The VPN Broker Gateway element represents the VPN Broker and contains information about the available endpoints.
- 3 The VPN Broker Domain is used to group all the VPN Broker members in a single domain.
- 4 A VPN Broker Member element represents each NGFW Engine.
- 5 The configuration file for the VPN Broker Domain is exported from the NGFW Manager.

Next steps

Begin the configuration in one of the following ways:

- If you need a custom Connectivity Type element, create a Connectivity Type element.
- Otherwise, create a VPN Broker Gateway element.

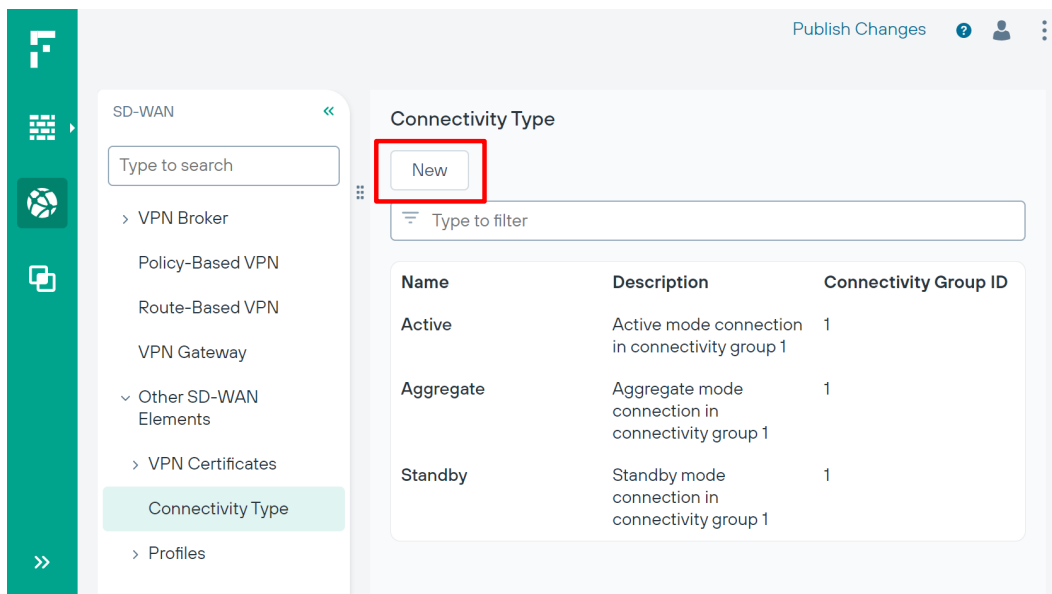
Create Connectivity Type elements in the NGFW Manager

Connectivity Type elements define the connectivity group to which endpoints belong, and the mode used when an endpoint is part of a Multi-Link configuration. If the default Connectivity Type elements meet your needs, it is not necessary to create custom Connectivity Type elements.

The default system Connectivity Type elements belong to connectivity group 1. If you need to use a different connectivity group, create a custom Connectivity Type element.

Steps

- 1) Browse to **SD-WAN > Other SD-WAN Elements > Connectivity Type**.



- 2) Click .

- 3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

Connectivity Type Properties	
Option	Definition
Mode	<p>Select one of the options to define how the endpoint is used in a Multi-Link configuration:</p> <ul style="list-style-type: none"> ▪ Active — The link is always used. If there are multiple links in Active mode between the Gateways, the VPN traffic is load-balanced between the links based on the load of the links. VPN traffic is directed to the link that has the lowest load. ▪ Aggregate — The link is always used, and each VPN connection is load-balanced in round-robin fashion between all the links that are in Aggregate mode. For example, if there are two links in Aggregate mode, a new VPN connection is directed to both links. ▪ Standby — The link is used only when all Active or Aggregate mode links are unusable.
Connectivity Group ID	Enter or select the number of the connectivity group to which the endpoint belongs. Tunnels are created only between endpoints that belong to the same connectivity group.
Link Type	This option is not yet supported.

Next steps

Create a VPN Broker Gateway element.

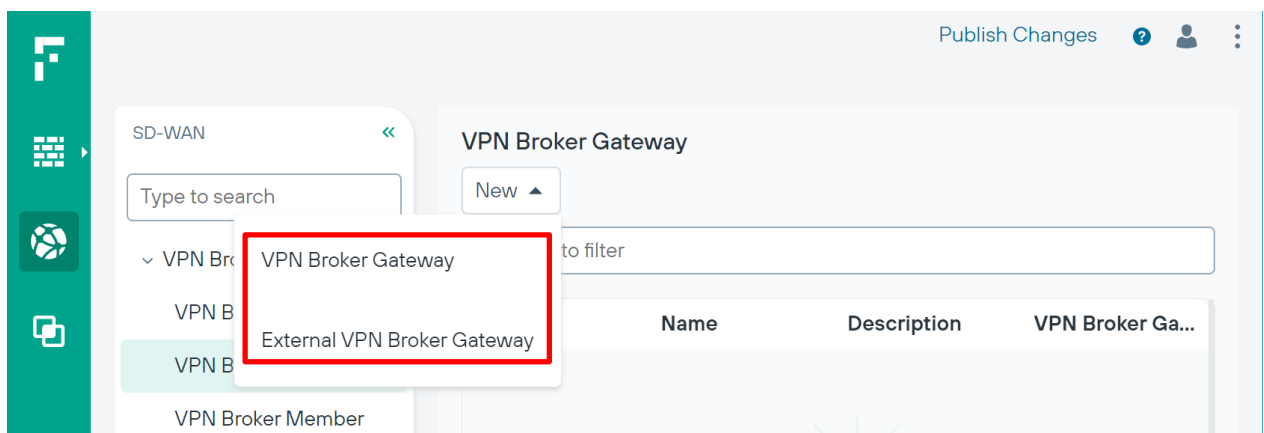
Create a VPN Broker Gateway element in the NGFW Manager

The VPN Broker Gateway element defines the endpoints used in the configuration.

The same VPN Broker gateway can belong to more than one VPN Broker domain.

Steps

- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Gateway**.



- 2) Click > **VPN Broker Gateway**.
- 3) Add a row in one of the following ways:
 - Click to add the first endpoint.

- Click ... > **New VPN Endpoint Before** to add an endpoint before the selected endpoint.
- Click ... > **New VPN Endpoint After** to add an endpoint after the selected endpoint.

4) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

VPN Broker Gateway properties	
Option	Definition
<p>Endpoints table</p> <p>To edit the contents of a cell, click the cell.</p> <p>Click ... > New VPN Endpoint Before or ... > New VPN Endpoint After to add a row.</p>	
Info	You can enter a name and a comment for the endpoint.
Endpoint Address	Select NGFW Engine IP Address , select Static Address , then select an element from the Static IP Address folder that represents the interface to use for the endpoint. Type part of the name of an element or browse through the drop-down list to select an element.
Endpoint Class	<p>Select a default system Connectivity Type element that has the appropriate mode selected. Type part of the name of an element or browse through the drop-down list to select an element.</p> <p>The following system Connectivity Type elements are available:</p> <ul style="list-style-type: none"> ■ Active — The link is always used. If there are multiple links in Active mode between the Gateways, the VPN traffic is load-balanced between the links based on the load of the links. VPN traffic is directed to the link that has the lowest load. ■ Aggregate — The link is always used, and each VPN connection is load-balanced in round-robin fashion between all the links that are in Aggregate mode. For example, if there are two links in Aggregate mode, a new VPN connection is directed to both links. ■ Standby — The link is used only when all Active or Aggregate mode links are unusable.
Used for Client Gateways	<p>When Yes is selected, VPN Broker members can communicate using the endpoint.</p> <p>If there is an intermediate NAT device between this VPN Broker and VPN Broker members, add a contact address.</p>
Used for Broker Servers	<p>When Yes is selected, other VPN Broker gateways can communicate using the endpoint.</p> <p>If there is an intermediate NAT device between this VPN Broker and other VPN Broker gateways, add a contact address.</p>

Option	Definition
VPN Broker Gateway ID	<p>Enter a unique ID number for the VPN Broker Gateway as an integer. The allowed range is 1–255.</p> <div data-bbox="451 254 506 310"> </div> <div data-bbox="537 254 1469 443"> <p>Note</p> <p>In the NGFW Manager, you enter the VPN Broker Gateway ID as a decimal number. However, the ID is converted internally to a hexadecimal number. For example, an ID of 10 is converted to 0A in the MAC address of the VPN Broker Gateway. The allowed range in hexadecimal numbers is 1–FF.</p> </div> <p>When a log entry is generated, the SMC uses this value to identify the VPN Broker that generated the log entry.</p> <div data-bbox="451 552 506 609"> </div> <div data-bbox="537 552 1469 680"> <p>Tip</p> <p>We recommend that you make a note of the VPN Broker Gateway ID for each VPN Broker Gateway.</p> </div> <div data-bbox="451 716 506 772"> </div> <div data-bbox="537 716 1469 821"> <p>Note</p> <p>With version 6.11, the VPN Broker is auto-populated.</p> </div>

Next steps

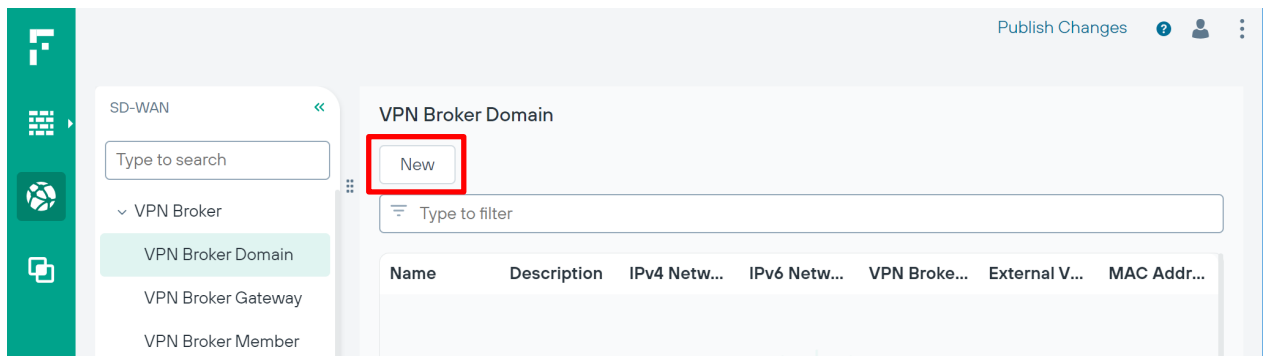
Create a VPN Broker Domain element.

Create a VPN Broker Domain element in the NGFW Manager

VPN Broker Domain element defines the virtual network that contains the VPN Broker gateway and the VPN Broker members.

Steps





- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Domain**.



- 2) Click .

3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

VPN Broker Domain properties	
Option	Definition
IPv4 Network or IPv6 Network	<p>Enter the IP address and netmask of the virtual network that contains all of the members of the VPN Broker domain. You must enter an IPv4 network, an IPv6 network, or both.</p> <p> Tip We recommend that you make a note of the IP addresses for each VPN Broker Domain.</p> <p> Note With version 6.11, IP address validation is done and notified to the administrator.</p>
VPN Broker Gateway	Select the VPN Broker Gateway that belongs to the VPN Broker domain. Type part of the name of an element or browse through the drop-down list to select an element.
External VPN Broker Gateways	This setting is used only in a VPN Broker high availability configuration.
MAC Address Prefix	<p>Enter a unique identifier for the VPN Broker Domain in MAC address format. The length must be three octets. The first octet must be even. The address must be a unique unicast MAC address.</p> <p> Tip We recommend that you make a note of the MAC Address Prefix for each VPN Broker Domain.</p> <p> Note With version 6.11, the MAC Address Prefix is auto-populated.</p>
Primary VPN Broker Server	This setting is used only in a VPN Broker high availability configuration.
Enabled	When selected, the VPN Broker Domain element is enabled. You can temporarily disable the element without deleting it.

Next steps

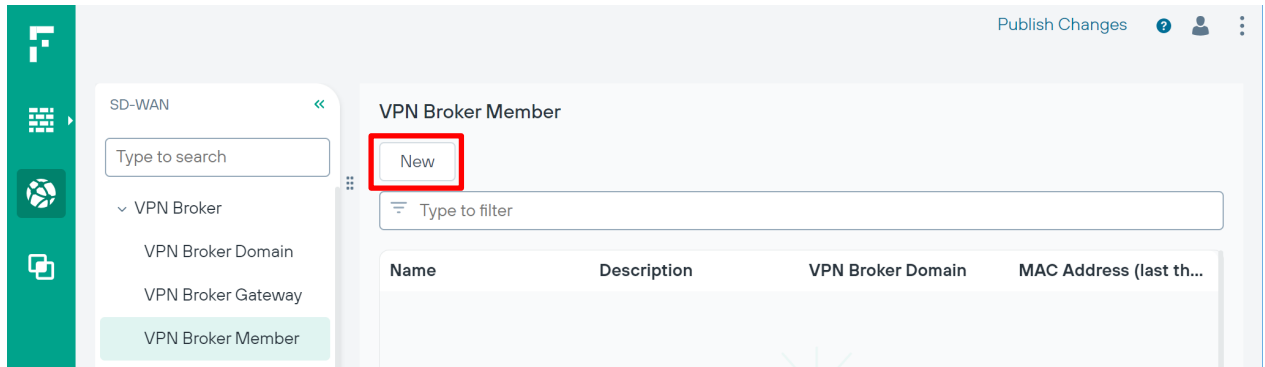
Create VPN Broker Member elements to represent each NGFW Engine that is used in the VPN Broker configuration.

Create VPN Broker Member elements in the NGFW Manager

Create VPN Broker Member elements to represent each NGFW Engine that is used in the VPN Broker configuration.

Steps

- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Member**.



- 2) Click .
- 3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

VPN Broker Member properties	
Option	Definition
VPN Broker Domain	Select the VPN Broker Domain element that you created. Type part of the name of an element or browse through the drop-down list to select an element.
Mac Address (last three octets)	<p>Enter a unique identifier for the VPN Broker Member as the last three octets of a MAC address. The allowed range is 00:01:00–ff:ff:ff. Each member in the domain must have a unique identifier. When adding a VPN Broker Interface to an NGFW Engine in the SMC, use the same value that is used in the corresponding VPN Broker Member element in the NGFW Manager.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Note</p> <p>The range 00:00:01– 00:00:FF is reserved for the VPN Broker Gateway element. You cannot use identifiers in this range for members in the domain.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <p>Tip</p> <p>We recommend that you make a note of the MAC addresses for each VPN Broker Member.</p> </div> <div style="border: 1px solid #ccc; padding: 5px;"> <p>Note</p> <p>With version 6.11, the MAC Address (last three octets) is auto-populated.</p> </div>

Option	Definition
Shared Secret	<p>Click Enter Shared Secret to enter a password. Click Change Shared Secret to change a password that has already been set.</p> <p>When adding a VPN Broker Interface to an NGFW Engine in the SMC, use the same value that is used in the corresponding VPN Broker Member element in the NGFW Manager.</p> <div data-bbox="451 359 492 411"> </div> <div data-bbox="537 359 1469 457"> <p>Tip</p> <p>We recommend that you make a note of the shared secret.</p> </div>
IPv4 Address or IPv6 Address	<p>Enter a member IP address that is part of the virtual network defined in the VPN Broker Domain element. You must enter an IPv4 address, an IPv6 address, or both.</p> <p>Use the same kind of IP address that the VPN Broker Domain uses. For example, if the VPN Broker Domain has only IPv4 addresses, enter an IPv4 address. You can enter both an IPv4 address and an IPv6 address if the VPN Broker Domain has both IPv4 addresses and IPv6 addresses.</p> <div data-bbox="451 716 492 768"> </div> <div data-bbox="537 716 1469 842"> <p>Tip</p> <p>We recommend that you make a note of the IP addresses for each VPN Broker Member.</p> </div> <div data-bbox="451 877 505 930"> </div> <div data-bbox="537 877 1469 976"> <p>Note</p> <p>With version 6.11, IP address validation is done and notified to the administrator.</p> </div>
<p>Networks table</p> <p>To edit the contents of a cell, click the cell.</p> <p>Click <input type="button" value="New"/> to add the first row.</p> <p>Click ⋮ > New Row Before or ⋮ > New Row After to add a row.</p>	
Network	<p>Select the networks that are reachable through the VPN Broker member. Type part of the name of an element or browse through the drop-down list to select an element.</p>
Mode	<p>Select from the following options.</p> <ul style="list-style-type: none"> ■ Reserved — Network addresses are dedicated to the gateway and these addresses or a subnet of these addresses cannot be given to any other member of the VPN Broker domain. This is the recommended option. ■ Allowed — Network addresses are allowed for the VPN gateway. However, the VPN Broker does not announce these as routes to other VPN gateways. Used for dynamic routing or the default VPN gateway. ■ Routed — When selected, enter a value in the Metric field. The same network address that has a different route metric value can be given to another VPN gateway. The subnet of a specified network can be given to a specified VPN gateway.

Next steps

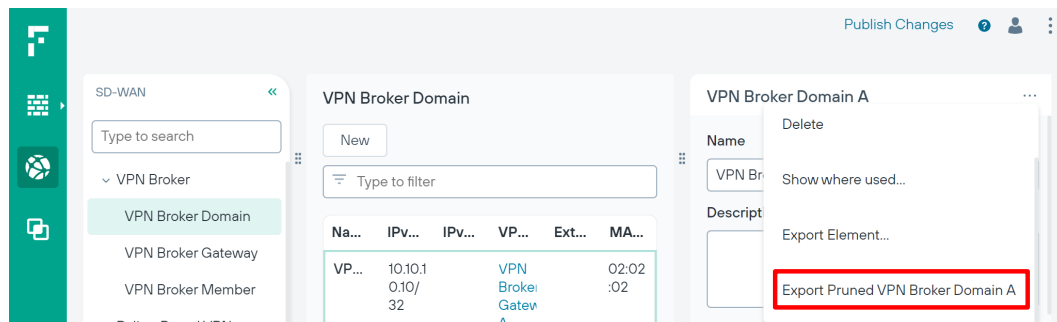
Export the VPN Broker Domain element to a file.

Export the VPN Broker Domain element to a file

To create the elements needed in the SMC, you must export the VPN Broker Domain element from the NGFW Manager.

Steps

- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Domain**.



- 2) Select the VPN Broker Domain element that you want to export, then click **⋮ > Export Pruned <name>**.
The **Export Pruned** option exports only the parts of the VPN Broker Domain configuration that are needed for creating a VPN Broker Domain element in the SMC. The exported configuration includes the VPN Broker Domain and the VPN Broker Members.
- 3) Save the .zip file to your local workstation.

Next steps

Enable the VPN configuration in the NGFW Manager.

Enable the VPN configuration in the NGFW Manager


The VPN configuration must be enabled in the properties of the NGFW Engine in the NGFW Manager.

Steps

- 1) Browse to **NGFW > Properties**.
- 2) Browse to the **VPN** section, then enable **VPN Configuration**.
- 3) To add a row to the **VPN Gateways** table, click **New**.

- 4) In the **VPN Gateway** cell, add the VPN Broker Gateway element that you created.
Type part of the name of an element or browse through the drop-down list to select an element.
- 5) Under **VPN Gateway Settings**, add the Gateway Default Settings element.
Type part of the name of an element or browse through the drop-down list to select an element.
- 6) Click **Save**.
- 7) If you have not yet viewed or edited the Access policy, at the top-right corner of the user interface click:
[Finalize the setup](#)
- 8) To publish your changes in the NGFW Manager, at the top-right corner of the user interface, click:
[Publish Changes](#)

Fields marked with an asterisk * in the user interface are mandatory.

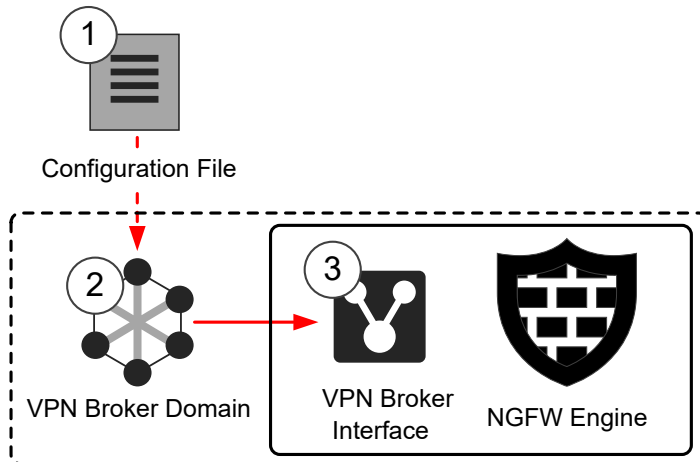
NGFW Engine Properties - VPN	
Option	Definition
VPN Configuration	When enabled, shows the VPN options.
VPN Gateways table	Shows the configured VPN gateways. To edit the contents of a cell, click the cell. Click  to add the first row. Click *** > New Row Before or *** > New Row After to add a row.
Gateway	The VPN Gateway element that represents the physical gateway device. Type part of the name of an element or browse through the drop-down list to select an element.
VPN Client Settings	This option is not yet supported.
SSL VPN Settings	This option is not yet supported.
Automatic Certificate Management	This option is not yet supported.
Automatic Sites From Routing	This option is not yet supported.
VPN Gateway Settings	The VPN Gateway Settings element defines performance-related VPN options. Type part of the name of an element or browse through the drop-down list to select an element.

Next steps

You have now finished the configuration steps in the NGFW Manager. Next, create elements for the VPN Broker configuration in the SMC.

Create elements for the VPN Broker configuration in the SMC

After you have finished the configuration steps in the NGFW Manager, you must create the elements that represent the VPN Broker configuration in the SMC.



- 1 The configuration file for the VPN Broker Domain is exported from the NGFW Manager.
- 2 The configuration file that you exported from the NGFW Manager is used in the VPN Broker Domain element.
- 3 The VPN Broker Interface is a virtual interface in the configuration of the NGFW Engine. The VPN Broker interface allows the NGFW Engine to act as a member of the VPN Broker domain.

Next steps

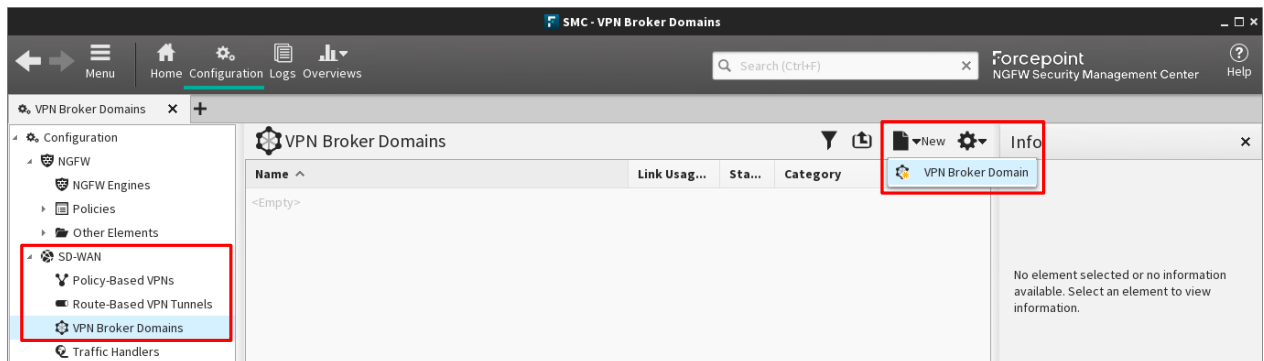
Begin by creating a VPN Broker Domain element in the SMC.

Create a VPN Broker Domain element in the SMC

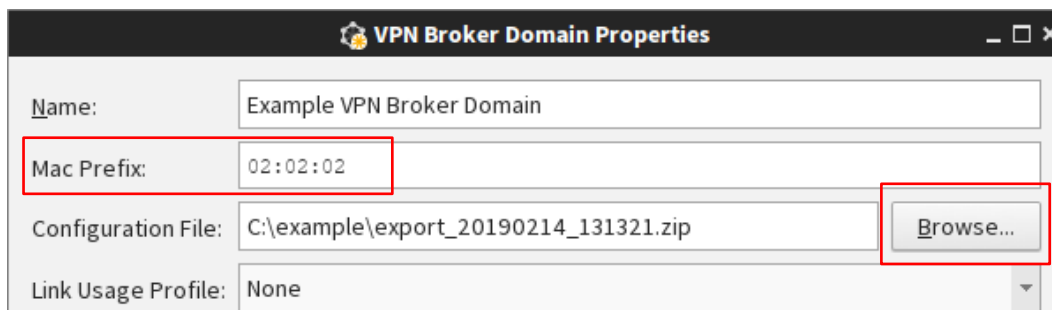
To create a VPN Broker Domain element in the SMC, you must use the exported configuration file from the NGFW Manager.

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

- 1) Open the Management Client.



- 2) Select **Configuration**, then browse to **SD-WAN**.
- 3) Browse to **VPN Broker Domains**.
- 4) Select **New > VPN Broker Domain**.



- 5) Configure the settings.
 - a) (Optional) Enter a name for the element.
If you do not enter a name, the name is automatically generated based on the name of the configuration file.
 - b) In the **Mac Prefix** field, enter the first three octets of the MAC address that is used by all members of the VPN Broker domain.
This MAC address prefix must be the same as the MAC address prefix that is used in the VPN Broker Domain element that you created in the NGFW Manager.

- c) Next to the **Configuration File** field, click **Browse**, then select the configuration file that you exported from the NGFW Manager.
- d) Click **OK**.


VPN Broker Domain properties	
Option	Definition
Name (Optional)	The name of the element.
Mac Prefix	Enter the first three octets of the MAC address that is used by all members of the VPN Broker domain. This MAC address prefix must be the same as the MAC address prefix that is used in the VPN Broker Domain element that you created in the NGFW Manager.
Configuration File	Click Browse to select the configuration file that you exported from the NGFW Manager.
Link Usage Profile (Optional)	To use dynamic link selection for Multi-Link VPNs, select a Link Usage Profile element. When you select a Link Usage Profile element in the properties of a policy-based VPN, route-based VPN tunnel group, or a VPN broker domain, the settings defined in the Link Usage Profile element are applied to all tunnels in the VPN according to their link types.

Next steps

Add a VPN Broker Interface to the NGFW Engine.

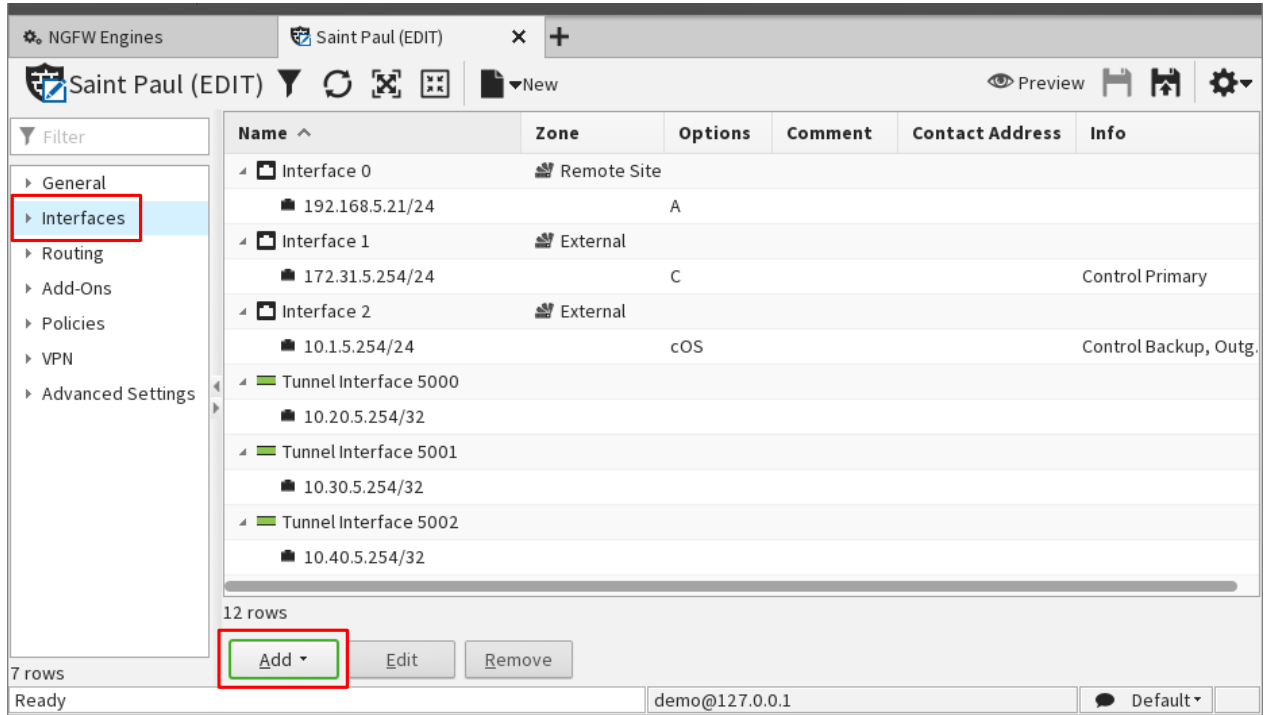
Add a VPN Broker Interface to the NGFW Engine

You must add a VPN Broker Interface to each NGFW Engine that is used as a VPN Broker member so that the VPN Broker can communicate with the members of a VPN Broker domain.

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

- 1) In the Management Client, select  **Configuration**.

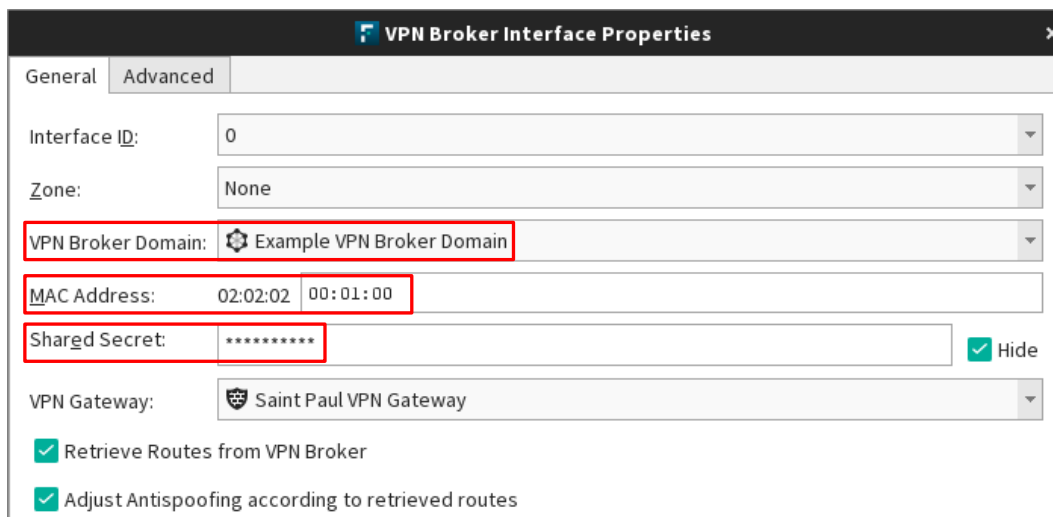
- 2) Right-click an NGFW Engine, then select **Edit <element type>**.



- 3) Browse to **Interfaces**.


- 4) Click **Add > VPN Broker Interface**.

- 5) Configure the settings.



- a) From the **VPN Broker Domain** drop-down list, select the VPN Broker Domain element that you created.
- b) In the **MAC Address** field, enter the last three octets of the MAC address for the VPN Broker member. This MAC address must be the same as the MAC address used in the corresponding VPN Broker Member element that you created in the NGFW Manager.

- c) In the **Shared Secret** field, enter the same password that you entered for the VPN Broker Member element in the NGFW Manager.
 - d) Click **OK**.
- 6) Right-click the VPN Broker Interface, then select **New > IPv4 Address** or **New > IPv6 Address**.
 - 7) Enter the IP address used in the corresponding VPN Broker Member element, then click **OK**.
 - 8) Click **Save and Refresh**, then click **OK** to transfer the changes to the NGFW Engine.

VPN Broker Interface properties	
Option	Definition
General tab	
Interface ID	The ID number that identifies the VPN Broker Interface. The VPN Broker Interface is a virtual interface that is used only for the VPN Broker. The interface ID of the VPN Broker Interface can be the same as the interface ID of a physical interface on the same NGFW Engine.
Zone (Optional)	Select the network zone to which the interface belongs. Click Select to select an element, or click New to create an element.
VPN Broker Domain	Select the VPN Broker Domain element that you created.
MAC Address	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;">  <p>Note The MAC address prefix for the VPN Broker Domain is automatically added based on the VPN Broker Domain element.</p> </div> <p>Enter the last three octets of the MAC address for the VPN Broker member. This MAC address must be the same as the MAC address used in the corresponding VPN Broker Member element that you created in the NGFW Manager.</p>
Shared Secret	Enter the password. The password must be the same as the shared secret that you entered for the VPN Broker Member element in the NGFW Manager. By default, passwords and keys are not shown in plain text. To show the password or key, deselect the Hide option.
VPN Gateway	Select the local VPN gateway.
Retrieve Routes from VPN Broker	When selected, the routing table is updated with routes that are retrieved by the VPN Broker.
Adjust Antispoofing according to retrieved routes	When selected, antispoofing rules are automatically adjusted based on the routes that are retrieved by the VPN Broker.
QoS Mode (Optional)	Defines how QoS is applied to the link on this interface. If Full QoS or DSCP Handling and Throttling is selected, a QoS policy must also be selected. If Full QoS is selected, the throughput must also be defined. If the interface is a Physical Interface, the same QoS mode is automatically applied to any VLANs created under it.

Option	Definition
<p>QoS Policy</p>	<p><i>(When QoS Mode is Full QoS or DSCP Handling and Throttling)</i></p> <p>The QoS policy for the link on this interface.</p> <p>If the interface is a Physical Interface, the same QoS policy is automatically selected for any VLANs created under it.</p> <div data-bbox="451 373 506 428" style="float: left; margin-right: 10px;"> </div> <div data-bbox="537 373 1468 531" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>If a Virtual Resource has a throughput limit defined, the interfaces on the Virtual NGFW Engine that use a QoS policy all use the same policy. The policy used in the first interface is used for all the interfaces.</p> </div>
<p>Interface Throughput Limit</p>	<p><i>(When QoS Mode is Full QoS)</i></p> <p>Enter the throughput for the link on this interface as megabits per second.</p> <p>If the interface is a Physical Interface, the same throughput is automatically applied to any VLANs created under it.</p> <p>The throughput is for uplink speed (outgoing traffic) and typically must correspond to the speed of an Internet link (such as an ADSL line), or the combined speeds of several such links when connected to a single interface.</p> <div data-bbox="451 846 506 900" style="float: left; margin-right: 10px;"> </div> <div data-bbox="537 846 1468 1031" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>CAUTION</p> <p>Make sure that you set the interface speed correctly. When the bandwidth is set, the NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. This scaling happens even if there are no bandwidth limits or guarantees defined for any traffic.</p> </div> <div data-bbox="451 1068 506 1123" style="float: left; margin-right: 10px;"> </div> <div data-bbox="537 1068 1468 1253" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>CAUTION</p> <p>The throughput for a Physical Interface for a Virtual NGFW Engine must not be higher than the throughput for the Master NGFW Engine interface that hosts the Virtual NGFW Engine. Contact the administrator of the Master NGFW Engine before changing this setting.</p> </div>
<p>MTU (Optional)</p>	<p>The maximum transmission unit (MTU) size on the connected link. Either enter a value between 400–65535 or select a common MTU value from the list.</p> <p>If the interface is a Physical Interface, the same MTU is automatically applied to any VLANs created under it.</p> <p>The default value (also the maximum standard MTU in Ethernet) is 1500. Do not set a value larger than the standard MTU, unless you know that all devices along the communication path support it.</p> <p>To set the MTU for a Virtual NGFW Engine, you must configure the MTU for the interface on the Master NGFW Engine that hosts the Virtual NGFW Engine, then refresh the policy on the Master NGFW Engine and the Virtual NGFW Engine.</p>

Next steps

Check the status of the VPN Broker.

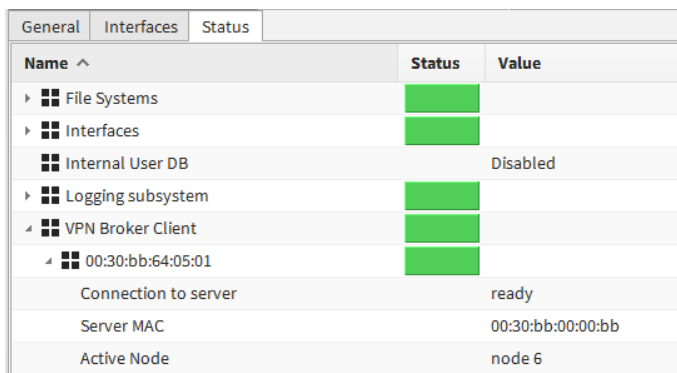
Check the status of the VPN Broker

To make sure that the components in the VPN Broker configuration are working correctly, check the status of the VPN Broker in the Management Client component of the SMC or on the command line of the NGFW Engine.

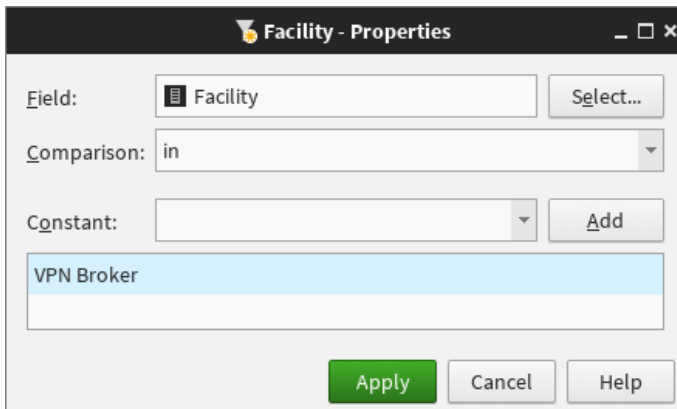
For more information about the monitoring features in the Management Client, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

- 1) Check the status in one or more of the following ways:
 - In the Home view of the Management Client, select an NGFW Engine to check the status of the connection between the NGFW Engine and the VPN Broker gateway. The **Status** tab of the **Info** pane shows the status.



- In the Logs view of the Management Client, use the VPN Broker facility in a filter to show logs related to the VPN Broker.



The following situations appear in log entries related to the VPN Broker:

Situation	Description
VPN-Broker_Client-Request	A VPN Broker member sent an information request to a VPN Broker gateway.
VPN-Broker_Connection_Error	The connection with the VPN Broker gateway has not been established.
VPN-Broker_Connection_Established	The connection with the VPN Broker gateway has been established.

- When VPN tunnels have been established between VPN Broker members, check the status of the tunnels in the SD-WAN dashboard in the Home view of the Management Client.

- On the command line of an NGFW Engine, enter the following command:

```
sg-brokerctl -s
```

On an NGFW Engine that acts as a VPN Broker gateway, the command shows a summary of the status of the connections between the VPN Broker members and the VPN Broker gateway. In a high availability environment, you can see if the VPN Broker gateways can be contacted. The age shown in the output should be 5 seconds or less. To check that the members have been synchronized correctly, you can enter `sg-brokerctl info` to check that the hash for `primary_member_hash` and `member_hash` match.

On an NGFW Engine that acts as a VPN Broker member, the command shows which other VPN Broker members the NGFW Engine can connect to, and shows the status of the connection between the NGFW Engine and the VPN Broker gateway.

Result

You have now finished configuring the VPN Broker.

Chapter 3

Configuring VPN Broker high availability

Contents

- Getting started with VPN Broker high availability on page 47
- VPN Broker high availability configuration overview on page 51
- Start the NGFW Manager on page 52
- Select the mode in the NGFW Manager on page 54
- Configure an interface for members of the VPN Broker domain on page 54
- Create elements for the VPN Broker high availability configuration in the NGFW Manager on page 57
- Export a VPN Broker Domain element to a file for high availability on page 67
- Enable the VPN configuration in each NGFW Manager on page 68
- Create elements for the VPN Broker high availability configuration in the SMC on page 70
- Check the status of the VPN Broker on page 76

When you configure high availability for the VPN Broker, there are multiple VPN Broker gateways in the same VPN Broker domain. All VPN Broker members can connect to any VPN Broker gateway in the VPN Broker domain.



Note

This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

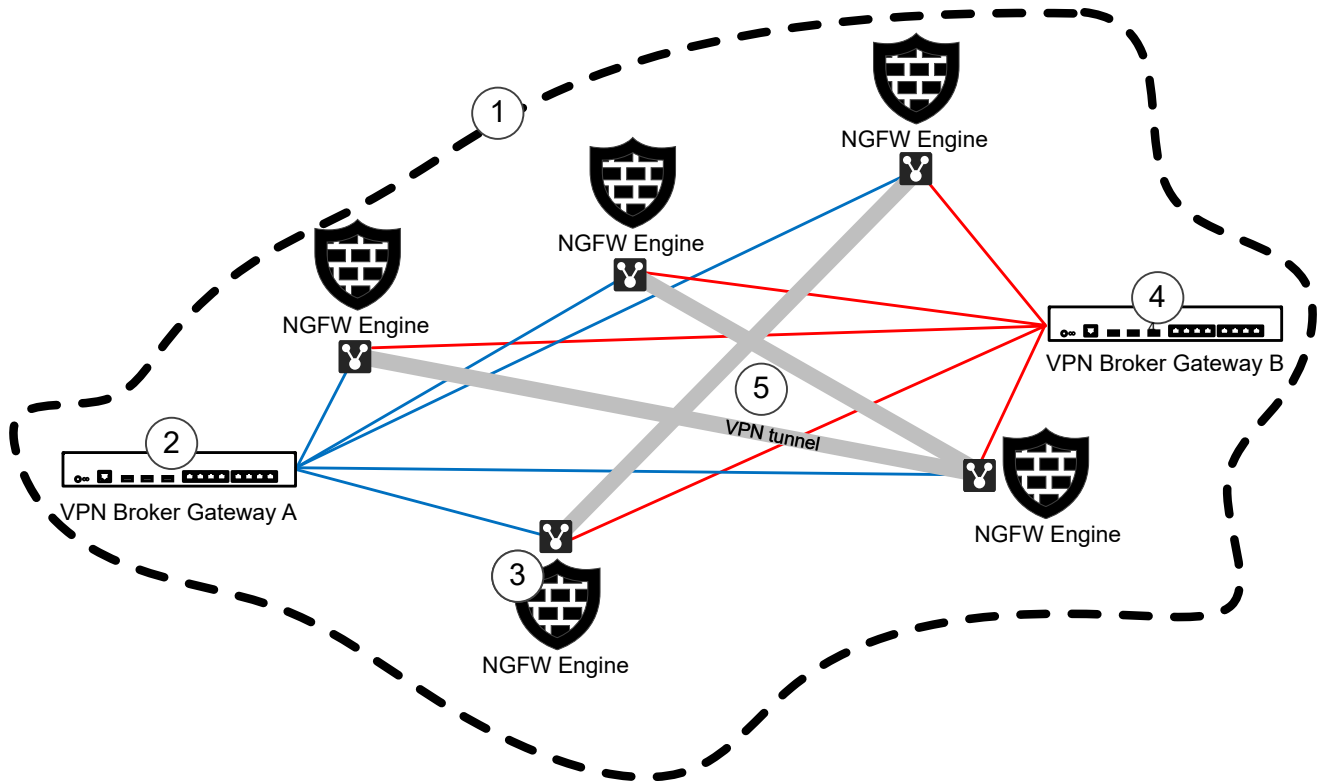
Getting started with VPN Broker high availability

The VPN Broker high availability environment consists of a VPN Broker domain, two or more VPN Broker gateways, and several VPN Broker members.

- VPN Broker domain — The VPN Broker domain is a virtual network that contains the VPN Broker gateways and the VPN Broker members.
- VPN Broker gateways — Each VPN Broker gateway is configured on a single pre-installed Forcepoint NGFW appliance that is dedicated for use only with the VPN Broker. When configuring the gateways in different instances of the NGFW Manager, set one as the primary gateway, and consider that NGFW Manager as the primary NGFW Manager. Changes that you make to the list of VPN Broker members in the primary NGFW Manager are automatically synchronized to other gateways.
- VPN Broker member — Each VPN Broker member is an NGFW Engine in the Firewall/VPN role (Single Firewall or Firewall Cluster). All VPN Broker members in the domain can connect to any VPN Broker gateway in the VPN Broker domain. When you use Master NGFW Engines and Virtual NGFW Engines, the same Master NGFW Engine can host VPN Broker members that belong to more than one VPN Broker domain.

VPN tunnels can be created between VPN Broker members that are controlled by different Management Servers. The members do not need to be in the same administrative Domain in the Forcepoint NGFW Security Management Center (SMC).

The following is an example environment for a VPN Broker high availability configuration. In this scenario, two VPN Broker gateways are configured in the same VPN Broker domain.



- 1 All VPN Broker members in the domain can connect to any VPN Broker gateway in the VPN Broker domain.
- 2 VPN Broker Gateway A
Communication between VPN Broker gateways in the domain is authenticated using a shared secret. This gateway has been configured in the primary NGFW Manager. Changes that you make to the list of VPN Broker members in the primary NGFW Manager are automatically synchronized to other gateways.
- 3 VPN Broker member
- 4 VPN Broker Gateway B
- 5 VPN tunnels are created and removed as needed between the VPN Broker members. The tunnels are negotiated using RSA authentication.

Access rules that allow communication between the VPN Broker gateway and the members are automatically created. The communication between VPN Broker members and the VPN Broker gateway is authenticated using a shared secret.

The members communicate with the VPN Broker gateways using a VPN Broker Interface that you must configure on each NGFW Engine. The traffic that goes into the VPN also passes through this interface.

VPN Broker gateway element types for VPN Broker high availability

In a VPN Broker high availability configuration, both VPN Broker Gateway and External VPN Broker Gateway elements are used.

- A VPN Broker Gateway element represents the local VPN Broker gateway in the NGFW Manager that manages it.
- An External VPN Broker Gateway element represents a remote VPN Broker gateway that is managed by a different NGFW Manager.

The same VPN Broker gateway is both a local VPN Broker gateway in its own configuration, and a remote VPN Broker gateway in the configurations of other VPN Broker gateways.

For example, VPN Broker Gateway A is managed by NGFW Manager A, and VPN Broker Gateway B is managed by NGFW Manager B. This table shows the element types that represent the VPN Broker gateways in each NGFW Manager.

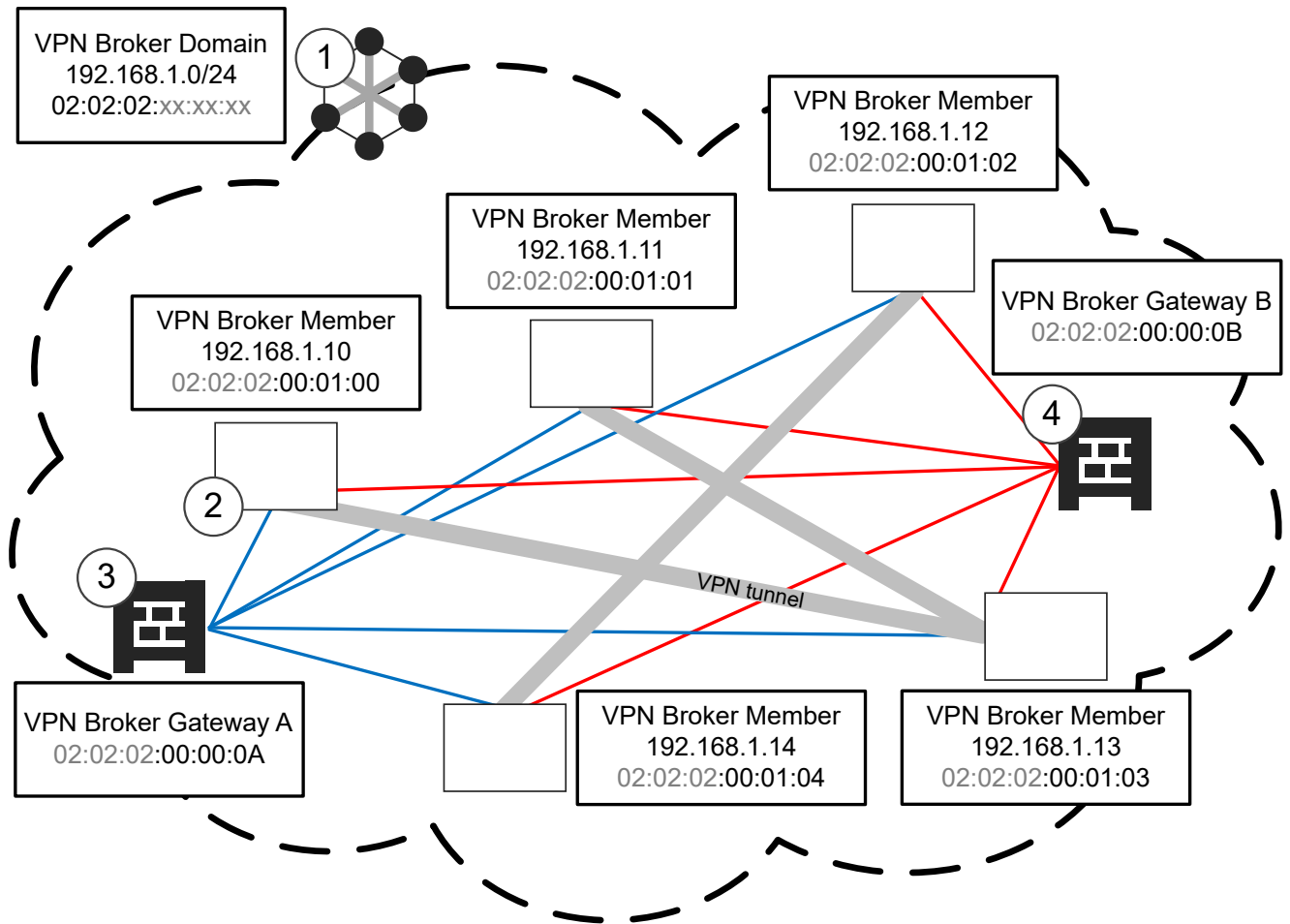
VPN Broker gateway element types

NGFW Manager	VPN Broker Gateway A	VPN Broker Gateway B
A	VPN Broker Gateway	External VPN Broker Gateway
B	External VPN Broker Gateway	VPN Broker Gateway

How the VPN Broker Domain works in a high availability environment

The VPN Broker domain is a virtual network that contains the VPN Broker gateway and the VPN Broker members.

The following is an example of IP addresses and MAC addresses in the VPN Broker Domain.



- 1 The VPN Broker Domain is a virtual network.
The VPN Broker Domain is identified by a unique MAC address prefix. In this example, the MAC address prefix is 02:02:02.
- 2 Each VPN Broker Member has an IP address that is part of the virtual network defined in the VPN Broker Domain.
Each VPN Broker Member is identified by a unique partial MAC address.
- 3 VPN Broker Gateway A is identified by a unique VPN Broker Gateway ID number. In this example, the VPN Broker Gateway ID is 10.
This gateway has been configured in the primary NGFW Manager. Changes that you make to the list of VPN Broker members in the primary NGFW Manager are automatically synchronized to other gateways.
- 4 The VPN Broker Gateway B is identified by a unique VPN Broker Gateway ID number. In this example, the VPN Broker Gateway ID is 11.

The MAC address prefix of the VPN Broker Domain is combined with the partial MAC address of each VPN Broker Member to form a complete MAC address for each VPN Broker Member.

Example of how VPN Broker Member MAC addresses are formed

MAC address prefix of the VPN Broker Domain	Partial MAC address of the VPN Broker Member	Complete MAC address of the VPN Broker Member
02:02:02	00:01:00	02:02:02:00:01:00
	00:01:01	02:02:02:00:01:01

MAC address prefix of the VPN Broker Domain	Partial MAC address of the VPN Broker Member	Complete MAC address of the VPN Broker Member
	00:01:02	02:02:02:00:01:02
	00:01:03	02:02:02:00:01:03
	00:01:04	02:02:02:00:01:04

The MAC address prefix of the VPN Broker Domain is combined with the VPN Broker Gateway ID number to form a complete MAC address for each VPN Broker Gateway.

In this example, the VPN Broker Gateway ID number for VPN Broker Gateway A is 10, and the VPN Broker Gateway ID number for VPN Broker Gateway B is 11. In the NGFW Manager, you enter the VPN Broker Gateway ID as a decimal number. However, the ID is converted internally to a hexadecimal number. For example, an ID of 10 is converted to 0A in the MAC address of the VPN Broker Gateway. An ID of 11 is converted to 0B in the MAC address of the VPN Broker Gateway.

How VPN Broker Gateway MAC addresses are formed

MAC address prefix of the VPN Broker Domain	VPN Broker Gateway ID	Complete MAC address of the VPN Broker Gateway
02:02:02	10	02:02:02:00:00:0A
	11	02:02:02:00:00:0B

VPN Broker high availability configuration overview

The configuration consists of these high-level steps.

Steps in the NGFW Manager

- 1) Start the NGFW Manager, then select VPN Broker Management mode.
- 2) In each NGFW Manager, configure the interface to which members of the VPN Broker domain can connect.
- 3) In each NGFW Manager, create the required elements in the following order:
 - a) One VPN Broker Gateway element to represent the local VPN Broker gateway.
 - b) External VPN Broker Gateway elements to represent all remote VPN Broker gateways.
 - c) One VPN Broker Domain element to which all VPN Broker gateways and external VPN Broker gateways belong.

When creating one of the VPN Broker Domain elements, you must set it to be the primary. Consider the NGFW Manager that you create the primary VPN Broker Domain element in as the primary NGFW Manager.

- 4) In the primary NGFW Manager, add VPN Broker Member elements.
Changes that you make to the list of VPN Broker members in the primary NGFW Manager are automatically synchronized to other gateways.
- 5) In the primary NGFW Manager, export the VPN Broker Domain element to a file.
- 6) In each NGFW Manager, enable the VPN configuration in the properties of the NGFW Engine.

Steps in the Management Client component of the SMC

- 1) Create the required elements in the following order:
 - a) Create one VPN Broker Domain element.
Import the VPN Broker Domain configuration file into the configuration of the VPN Broker Domain element.
 - b) Add a VPN Broker Interface to all NGFW Engines that are used as VPN Broker members.
- 2) Refresh the firewall policy.



Note

VPN Broker provides connectivity between networks of the VPN Broker members. You must add Access rules to the policy of each NGFW Engine to allow specific types of traffic to and from these networks.

Begin the configuration by starting the NGFW Manager.

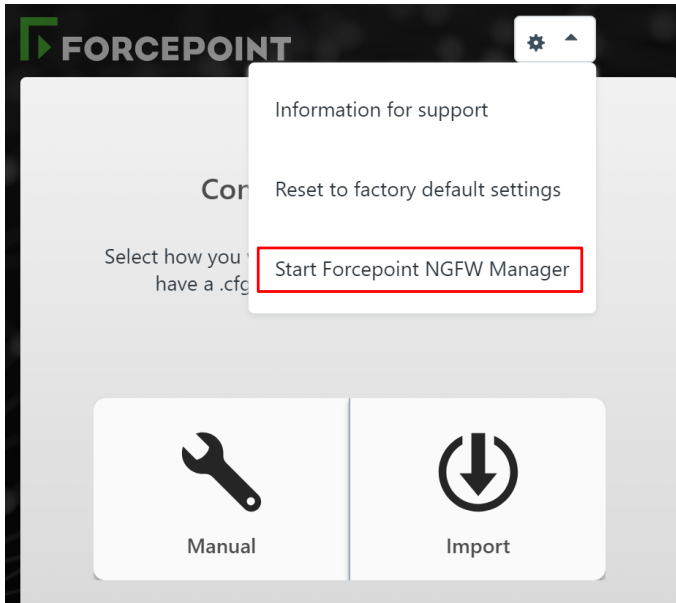
Start the NGFW Manager

The NGFW Configuration Wizard allows you to configure settings for the Forcepoint NGFW appliance. Start the NGFW Manager from the web browser version of the NGFW Configuration Wizard.

Steps

- 1) Connect the NGFW appliance to a laptop or other client device.
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) Connect the other network cables to the Forcepoint NGFW appliance.
- 3) Turn on the Forcepoint NGFW appliance.
- 4) To start the web browser version of the NGFW Configuration Wizard, open a web browser on the client device, then connect to <https://169.254.169.169>.
It might take some time for the web page to load.

- 5) When the NGFW Configuration Wizard offers a web browser client certificate, accept the certificate.
- 6) On the Welcome page of the NGFW Configuration Wizard, click **Start**.
- 7) Select **I Agree to the Terms and Conditions**, then click **Next**.
- 8) Enter and confirm the password for the root account, then click **Next**.



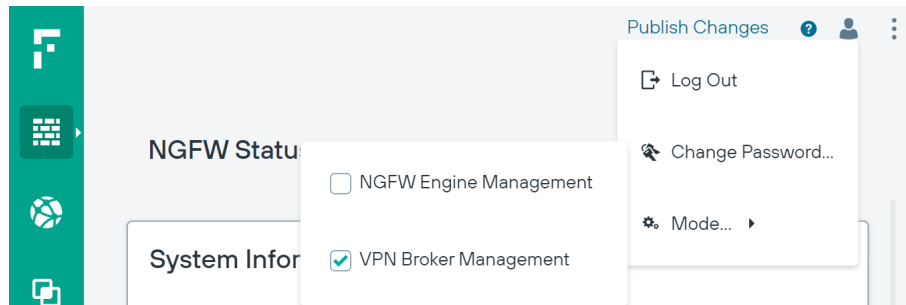
- 9) Click **⚙** > **Start Forcepoint NGFW Manager** to restart the appliance.
- 10) After the NGFW appliance has restarted, refresh the web browser to start the NGFW Manager.
- 11) Enter `root` as the user name, enter the password for the root account, then click **Log In**.

Next steps

Continue by selecting the mode in the NGFW Manager.

Select the mode in the NGFW Manager

Modes in the NGFW Manager allow you to either configure the VPN Broker or locally manage a single NGFW Engine.



Steps

- 1) Select **User** > **Mode**, then select the mode.
 - **VPN Broker Management** — Allows you to configure the VPN Broker. In this mode, elements and options related to the VPN Broker are shown in addition to elements and options related to the management of the NGFW Engine.
 - **NGFW Engine Management** — Allows you to locally manage a single NGFW Engine. In this mode, elements and options related to the VPN Broker are not shown.



Note

If you are in the **VPN Broker** branch of the **SD-WAN** view, you cannot change the mode to **NGFW Engine Management**. Browse to a different view, then change the mode.

Next steps

Continue the configuration in one of the following ways:

- If you are configuring the VPN Broker, configure an interface for members of the VPN Broker domain.
- If you are locally managing a single NGFW Engine, create elements to use for NGFW Engine configuration.

Configure an interface for members of the VPN Broker domain

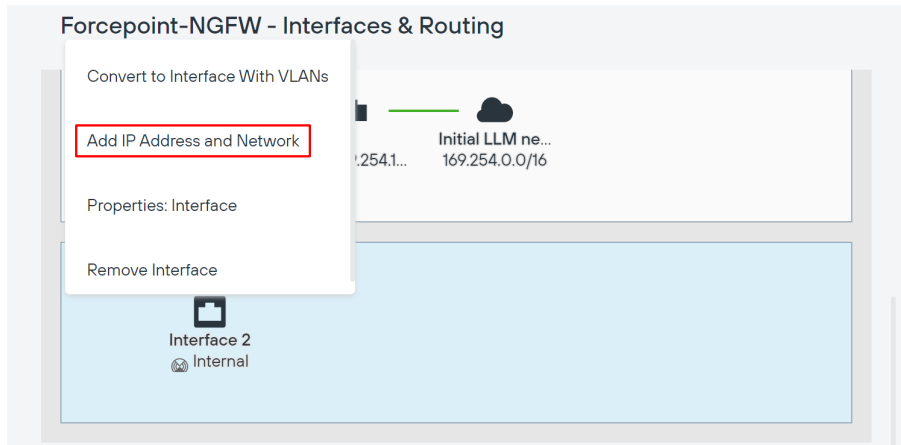
Interfaces for each Ethernet port on the NGFW appliance are automatically included in the interface table. In each NGFW Manager, you must add an IP address for the interface to which members of the VPN Broker domain can connect.

Before you begin

Start the NGFW Manager, then select VPN Broker Management mode.

Steps

- 1) Browse to **NGFW > Interfaces**.



- 2) In the interface table below the appliance image, click an interface, then select **Add IP Address and Network**.
- 3) Enter the IP address and netmask to which members of the VPN Broker domain can connect in CIDR notation, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

Interfaces & Routing page	
Option	Definition
<input type="button" value="New"/>	<p>Adds an interface to the interfaces table. If you change the number of Ethernet ports on the NGFW appliance, such as by replacing a 4-port interface module with an 8-port interface module, you must add interfaces to represent the new Ethernet ports.</p> <ul style="list-style-type: none"> ■ Interface — Adds a physical interface. Opens the New Interface pane. ■ Interface with VLANs — Adds a physical interface with a placeholder for adding VLAN interfaces later. Opens the New Interface With VLANs pane. ■ Tunnel Interface — This option is not yet supported.
Appliance image	Shows the ports on the NGFW appliance for which you can configure interfaces. When you select an interface in the interface table, the corresponding port is highlighted in the image.
Interface table	Allows you to configure the IP addresses, networks, and routing for each interface.
Physical Interface	<p><i>(When interface type is Physical Interface)</i></p> <p>Shows the interface ID of the physical interfaces. The following actions are available when you click the interface:</p> <ul style="list-style-type: none"> ■ Add IP Address and Network — Adds an IP address and a Network element to the interface. Opens the New IP Address and Netmask pane. ■ Convert to Interface With VLANs — Removes any IP addresses that have been specified and converts the interface to an interface with VLANs. ■ Properties: Interface — Opens the interface properties. ■ Remove Interface — Removes the interface from the configuration.

Option	Definition
Physical Interface	<p><i>(When interface type is Physical Interface with VLAN interfaces)</i></p> <p>Shows the interface ID of the physical interfaces and the VLAN interfaces under them. The following actions are available when you click the physical interface:</p> <ul style="list-style-type: none"> ■ Add VLAN Interface — Adds a VLAN interface. ■ Convert to Interface — Converts the interface with VLANs to an interface. There can be a maximum of one VLAN Interface when you convert the interface. ■ Properties: Interface with VLANs — Opens the interface properties. ■ Remove Interface — Removes the interface from the configuration. <p>The following actions are available when you click the VLAN interface:</p> <ul style="list-style-type: none"> ■ Add IP Address and Network — Adds an IP address and a Network element to the interface. Opens the New IP Address and Netmask pane. ■ Properties: VLAN Interface — Opens the VLAN interface properties. ■ Remove VLAN Interface — Removes the VLAN interface.
IP Address	<p>Shows the IP address of the physical interface or VLAN interface. The following actions are available when you click the IP address:</p> <ul style="list-style-type: none"> ■ Properties: Static Address — Allows you to add a static IP address to the interface. ■ Remove IP Address and Network — Removes the IP address from the interface configuration.
Connected Network	<p>Shows the network range of the directly connected network. The following options are available when you click the network:</p> <ul style="list-style-type: none"> ■ Add Gateway — Allows you to add a route through a gateway device to a network that is not directly connected. ■ Properties: Network — Opens the properties of the Network element.
Gateway	<p>Shows the gateway device through which the NGFW Engine connects to a network that is not directly connected. The following actions are available when you click the gateway:</p> <ul style="list-style-type: none"> ■ Add Route Target — Allows you to specify the IP addresses that are reachable through the gateway device. ■ Properties: <element type> — Opens the properties of the element that represents the gateway device. ■ Remove Gateway — Removes the gateway device from the interface configuration. The element is not deleted.
Route Target	<p>Shows the IP addresses that are reachable through the gateway device. The following options are available when you click the route target:</p> <ul style="list-style-type: none"> ■ Properties: <element type> — Opens the properties of the element that represents the IP addresses. ■ Remove Route Target — Removes the route target from the interface configuration. The element is not deleted.

Interface properties	
Option	Definition
Interface ID	<p><i>(When interface type is Physical Interface)</i></p> <p>The Interface ID automatically maps to a physical network port on the appliance.</p>

Option	Definition
VLAN ID	<i>(When interface type is VLAN Interface)</i> Specifies the VLAN ID (1–4094). The VLAN IDs must be the same as the VLAN IDs that are used in the switch at the other end of the VLAN trunk. Each VLAN Interface is identified as Interface-ID.VLAN-ID, for example, 2.100 for Interface ID 2 and VLAN ID 100.
Interface Options (Optional)	Advanced options for interface configuration.
MTU	The maximum transmission unit (MTU) size on the connected link. Enter a value between 576–65000.
Zone	The network zone to which the interface belongs. By default, Interface 0 belongs to the external zone. All other interfaces belong to the internal zone.
Log Compression Override	When selected, the log compression settings defined for the interface override the default log compression settings defined for the NGFW Engine. <ul style="list-style-type: none"> ■ Compress Discard Logs — When selected, enables log compression for discard log entries. ■ Compress Antispoofing Logs — When selected, enables log compression for antispoofing log entries.
Log Rate	The maximum sustained number of log entries per second. The default value is 100 log entries per second.
Log Burst Size	The maximum number of log entries in a single burst. The default value is 1000 log entries.
Antispoofing Elements	This option is not yet supported.
Route Replies Back	This option is not yet supported.

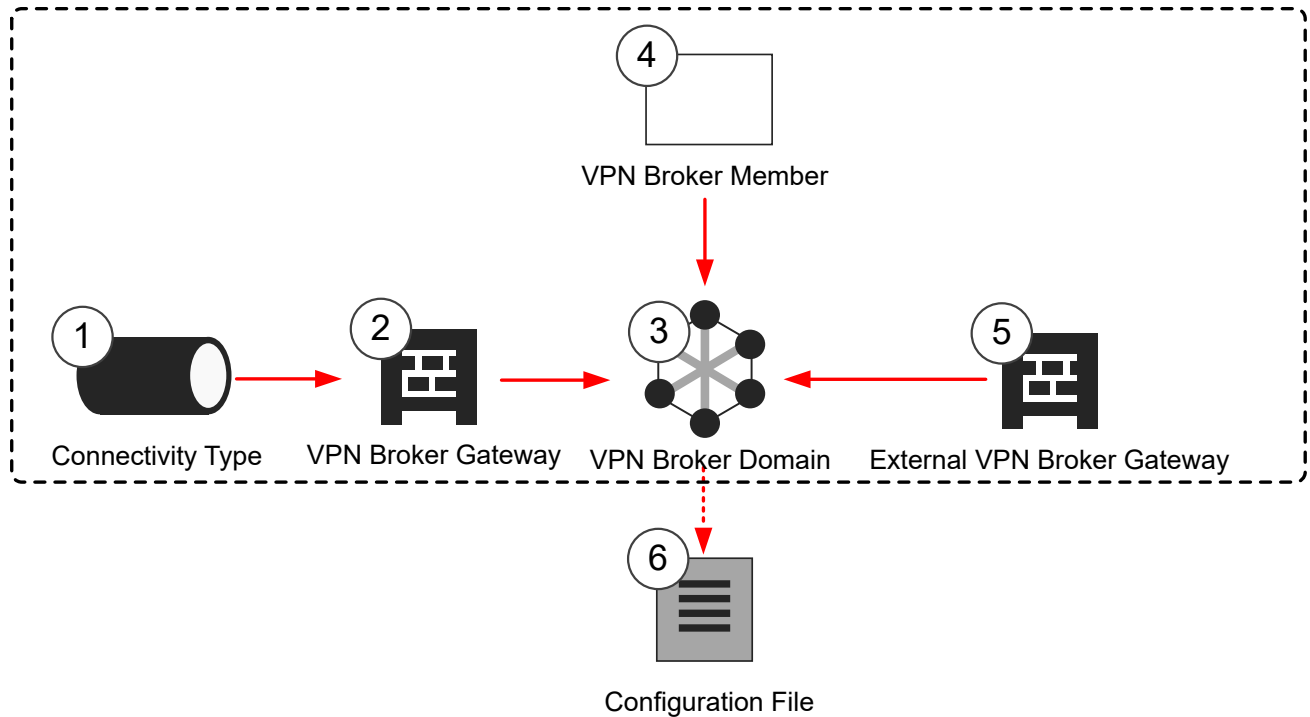
Next steps

Create elements for the VPN Broker configuration in the NGFW Manager.

Create elements for the VPN Broker high availability configuration in the NGFW Manager

You must create the elements that represent the VPN Broker configuration in the NGFW Manager.

The following elements are used in the configuration:



- 1 Connectivity Type elements define the connectivity group to which endpoints belong, and the mode used when an endpoint is part of a Multi-Link configuration.
The default system Connectivity Type elements belong to connectivity group 1. If you need to use a different connectivity group, create a custom Connectivity Type element.
- 2 The VPN Broker Gateway element represents the local VPN Broker and contains information about the available endpoints.
- 3 The VPN Broker Domain is used to group all the VPN Broker members in a single domain.
You must create an identical VPN Broker Domain element in each NGFW Manager.
- 4 Each VPN Broker Member element represents an NGFW Engine.
- 5 Each External VPN Broker Gateway element represents a remote VPN Broker.
- 6 The configuration file for one VPN Broker Domain is exported from the NGFW Manager.

Next steps

Begin the configuration in one of the following ways:

- If you need a custom Connectivity Type element, create a Connectivity Type element.
- Otherwise, create a VPN Broker Gateway element to represent the local VPN Broker.

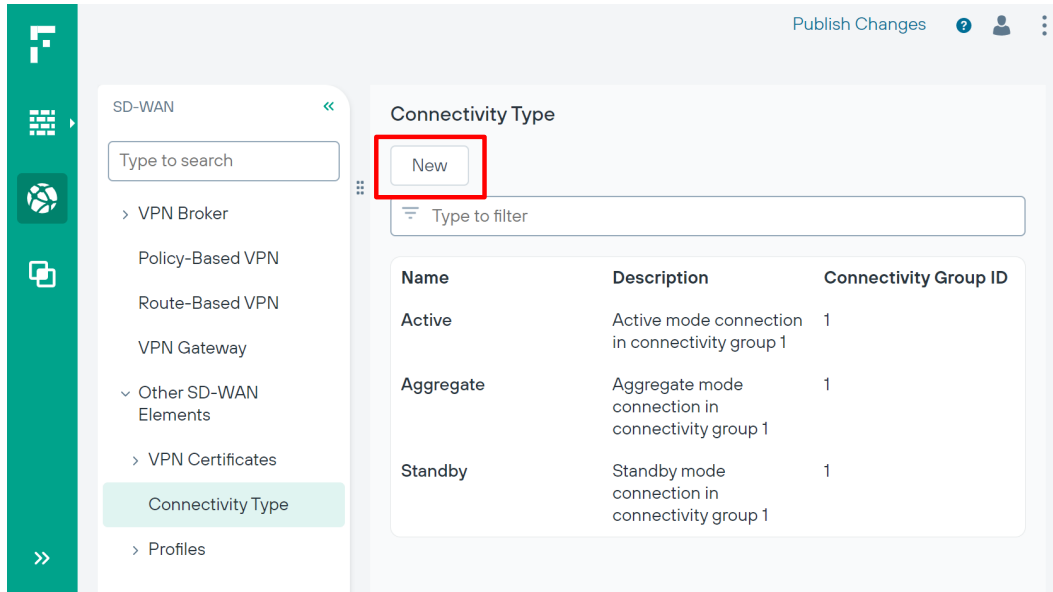
Create Connectivity Type elements in the NGFW Manager

Connectivity Type elements define the connectivity group to which endpoints belong, and the mode used when an endpoint is part of a Multi-Link configuration. If the default Connectivity Type elements meet your needs, it is not necessary to create custom Connectivity Type elements.

The default system Connectivity Type elements belong to connectivity group 1. If you need to use a different connectivity group, create a custom Connectivity Type element.

Steps

- 1) Browse to **SD-WAN > Other SD-WAN Elements > Connectivity Type**.



- 2) Click .
- 3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

Connectivity Type Properties	
Option	Definition
Mode	Select one of the options to define how the endpoint is used in a Multi-Link configuration: <ul style="list-style-type: none"> ■ Active — The link is always used. If there are multiple links in Active mode between the Gateways, the VPN traffic is load-balanced between the links based on the load of the links. VPN traffic is directed to the link that has the lowest load. ■ Aggregate — The link is always used, and each VPN connection is load-balanced in round-robin fashion between all the links that are in Aggregate mode. For example, if there are two links in Aggregate mode, a new VPN connection is directed to both links. ■ Standby — The link is used only when all Active or Aggregate mode links are unusable.
Connectivity Group ID	Enter or select the number of the connectivity group to which the endpoint belongs. Tunnels are created only between endpoints that belong to the same connectivity group.
Link Type	This option is not yet supported.

Next steps

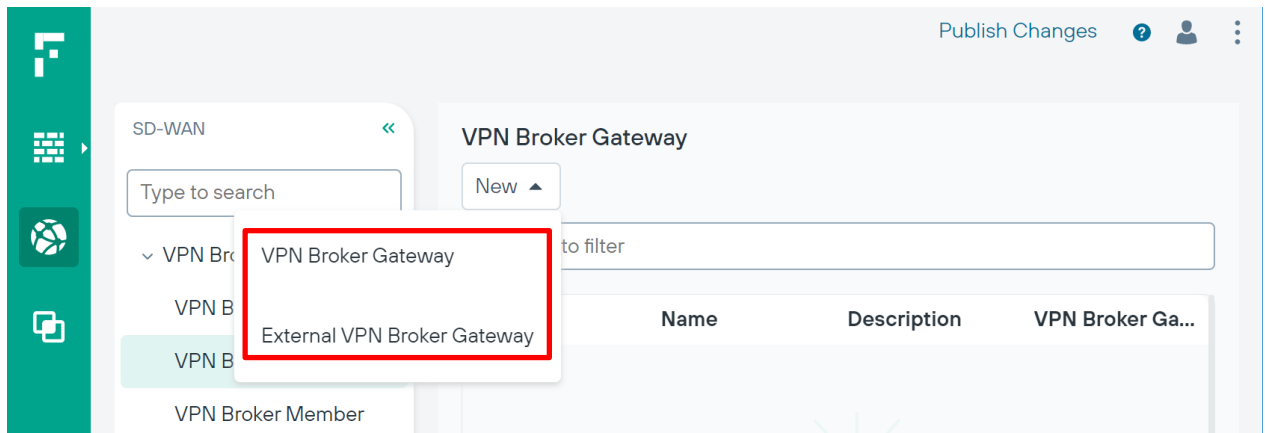
Create a VPN Broker Gateway element.

Create a local VPN Broker Gateway element for VPN Broker high availability

In each NGFW Manager, create one VPN Broker Gateway element to represent the local VPN Broker gateway.

Steps




- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Gateway**.



- 2) Click > **VPN Broker Gateway**.
- 3) Add a row in one of the following ways:
 - Click to add the first endpoint.
 - Click **...** > **New VPN Endpoint Before** to add an endpoint before the selected endpoint.
 - Click **...** > **New VPN Endpoint After** to add an endpoint after the selected endpoint.
- 4) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

VPN Broker Gateway properties	
Option	Definition
Endpoints table To edit the contents of a cell, click the cell. Click ... > New VPN Endpoint Before or ... > New VPN Endpoint After to add a row.	
Info	You can enter a name and a comment for the endpoint.
Endpoint Address	Select NGFW Engine IP Address , select Static Address , then select an element from the Static IP Address folder that represents the interface to use for the endpoint. Type part of the name of an element or browse through the drop-down list to select an element.

Option	Definition
Endpoint Class	<p>Select a default system Connectivity Type element that has the appropriate mode selected. Type part of the name of an element or browse through the drop-down list to select an element.</p> <p>The following system Connectivity Type elements are available:</p> <ul style="list-style-type: none"> ■ Active — The link is always used. If there are multiple links in Active mode between the Gateways, the VPN traffic is load-balanced between the links based on the load of the links. VPN traffic is directed to the link that has the lowest load. ■ Aggregate — The link is always used, and each VPN connection is load-balanced in round-robin fashion between all the links that are in Aggregate mode. For example, if there are two links in Aggregate mode, a new VPN connection is directed to both links. ■ Standby — The link is used only when all Active or Aggregate mode links are unusable.
Used for Client Gateways	<p>When Yes is selected, VPN Broker members can communicate using the endpoint. If there is an intermediate NAT device between this VPN Broker and VPN Broker members, add a contact address.</p>
Used for Broker Servers	<p>When Yes is selected, other VPN Broker gateways can communicate using the endpoint. If there is an intermediate NAT device between this VPN Broker and other VPN Broker gateways, add a contact address.</p>
VPN Broker Gateway ID	<p>Enter a unique ID number for the VPN Broker Gateway as an integer. The allowed range is 1–255.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Note</p> <p>In the NGFW Manager, you enter the VPN Broker Gateway ID as a decimal number. However, the ID is converted internally to a hexadecimal number. For example, an ID of 10 is converted to 0A in the MAC address of the VPN Broker Gateway. The allowed range in hexadecimal numbers is 1–FF.</p> </div> <p>When a log entry is generated, the SMC uses this value to identify the VPN Broker that generated the log entry.</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Tip</p> <p>We recommend that you make a note of the VPN Broker Gateway ID for each VPN Broker Gateway.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p> Note</p> <p>With version 6.11, the VPN Broker is auto-populated.</p> </div>

Next steps

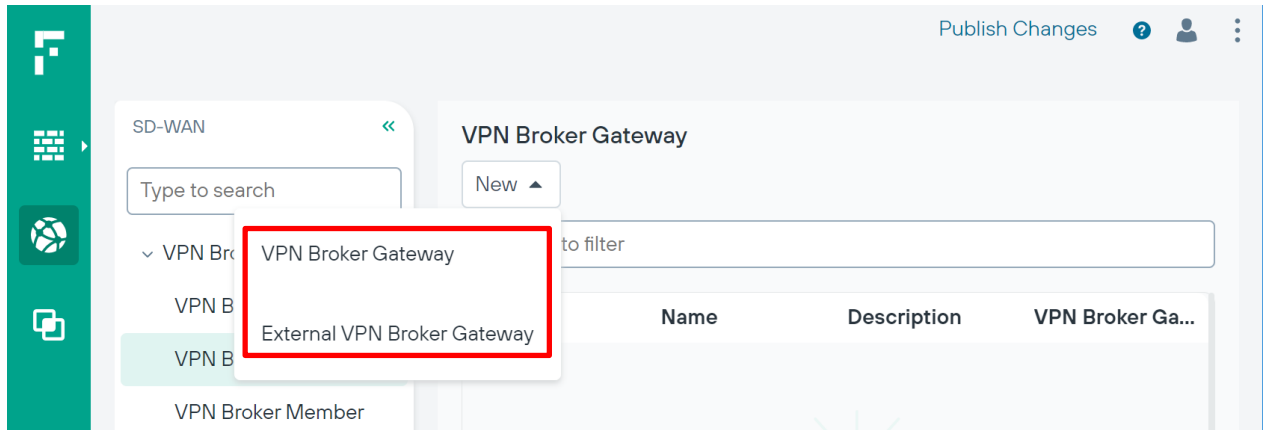
Create External VPN Broker Gateway elements to represent all remote VPN Broker gateways.

Create External VPN Broker Gateway elements for VPN Broker high availability

External VPN Broker Gateways are remote VPN Broker gateways that are managed by a different NGFW Manager. You must create one External VPN Broker Gateway element to represent each remote VPN Broker gateway in each NGFW Manager.

Steps

1) Browse to **SD-WAN > VPN Broker > VPN Broker Gateway**.



2) Click > **External VPN Broker Gateway**.

3) Add a row in one of the following ways:

- Click to add the first endpoint.
- Click **...** > **New VPN Endpoint Before** to add an endpoint before the selected endpoint.
- Click **...** > **New VPN Endpoint After** to add an endpoint after the selected endpoint.

4) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

External VPN Broker Gateway properties	
Option	Definition
Endpoints table To edit the contents of a cell, click the cell. Click ... > New VPN Endpoint Before or ... > New VPN Endpoint After to add a row.	
Info	You can enter a name and a comment for the endpoint.
Endpoint Address	Enter the IP address of the remote gateway.
Endpoint Class	Select a default system Connectivity Type element that has the appropriate mode selected. Type part of the name of an element or browse through the drop-down list to select an element. The following system Connectivity Type elements are available: <ul style="list-style-type: none"> ■ Active — The link is always used. If there are multiple links in Active mode between the Gateways, the VPN traffic is load-balanced between the links based on the load of the links. VPN traffic is directed to the link that has the lowest load. ■ Aggregate — The link is always used, and each VPN connection is load-balanced in round-robin fashion between all the links that are in Aggregate mode. For example, if there are two links in Aggregate mode, a new VPN connection is directed to both links. ■ Standby — The link is used only when all Active or Aggregate mode links are unusable.

Option	Definition
Used for Client Gateways	When Yes is selected, VPN Broker members can communicate using the endpoint. If there is an intermediate NAT device between this VPN Broker and VPN Broker members, add a contact address.
Used for Broker Servers	When Yes is selected, external VPN Broker gateways can communicate using the endpoint. If there is an intermediate NAT device between this VPN Broker and other VPN Broker gateways, add a contact address.
Shared Secret	<p>To specify the shared secret that VPN Broker Gateways use to authenticate each other in a high availability configuration, click Shared Secret, enter the shared secret, then click Save.</p> <div data-bbox="451 520 490 571"></div> <div data-bbox="548 527 591 556">Tip</div> <div data-bbox="548 571 1175 600">We recommend that you make a note of the shared secret.</div> <div data-bbox="451 655 506 705"></div> <div data-bbox="548 663 607 693">Note</div> <div data-bbox="548 707 1440 766">Enter the same shared secret in the properties of each VPN Broker Gateway in the same VPN Broker Domain.</div>
VPN Broker Gateway ID	<p>Enter a unique ID number for the VPN Broker Gateway as an integer. The allowed range is 1–255.</p> <div data-bbox="451 877 506 928"></div> <div data-bbox="548 888 607 917">Note</div> <div data-bbox="548 932 1455 1050">In the NGFW Manager, you enter the VPN Broker Gateway ID as a decimal number. However, the ID is converted internally to a hexadecimal number. For example, an ID of 10 is converted to 0A in the MAC address of the VPN Broker Gateway. The allowed range in hexadecimal numbers is 1–FF.</div> <p>When a log entry is generated, the SMC uses this value to identify the VPN Broker that generated the log entry.</p> <div data-bbox="451 1176 490 1226"></div> <div data-bbox="548 1186 591 1215">Tip</div> <div data-bbox="548 1230 1440 1289">We recommend that you make a note of the VPN Broker Gateway ID for each VPN Broker Gateway.</div> <div data-bbox="451 1344 506 1394"></div> <div data-bbox="548 1354 607 1383">Note</div> <div data-bbox="548 1398 1110 1428">With version 6.11, the VPN Broker is auto-populated.</div>

Next steps

Create identical VPN Broker Member elements in each NGFW Manager.

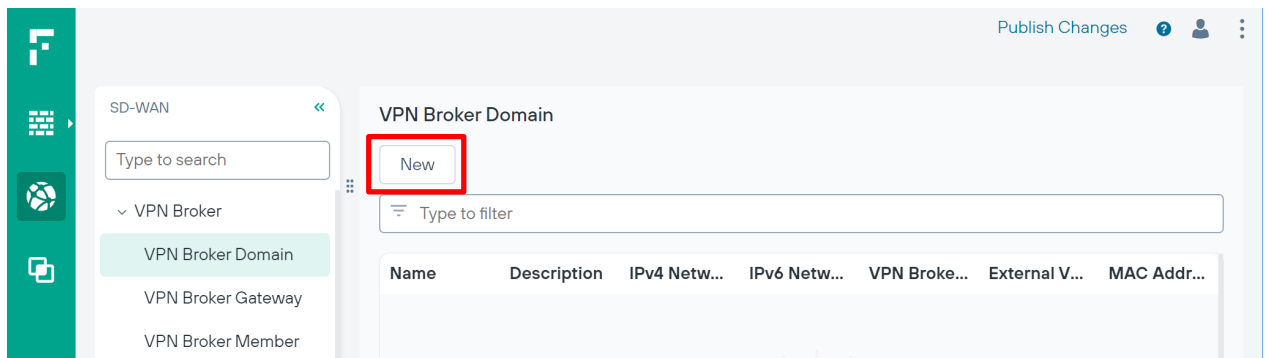
Create VPN Broker Domain elements for VPN Broker high availability

The VPN Broker Domain element defines the virtual network that contains the local and remote VPN Broker gateways, and the VPN Broker domain members.

Create a VPN Broker Domain element in each NGFW Manager. When creating one of the VPN Broker Domain elements, you must set it to be the primary. Consider the NGFW Manager that you create the primary VPN Broker Domain element in as the primary NGFW Manager. Changes that you make to the list of VPN Broker members in the primary NGFW Manager are automatically synchronized to other gateways.



Steps



- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Domain**.



- 2) Click .
- 3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

VPN Broker Domain properties	
Option	Definition
IPv4 Network or IPv6 Network	<p>Enter the IP address and netmask of the virtual network that contains all of the members of the VPN Broker domain. You must enter an IPv4 network, an IPv6 network, or both.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Tip</p> <p>We recommend that you make a note of the IP addresses for each VPN Broker Domain.</p> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>With version 6.11, IP address validation is done and notified to the administrator.</p> </div>
VPN Broker Gateway	Select the local VPN Broker Gateway that belongs to the VPN Broker domain. Type part of the name of an element or browse through the drop-down list to select an element.
External VPN Broker Gateways	Select all External VPN Broker Gateways that belong to the VPN Broker domain. Type part of the name of an element or browse through the drop-down list to select an element.

Option	Definition
MAC Address Prefix	<p>Enter a unique identifier for the VPN Broker Domain in MAC address format. The length must be three octets. The first octet must be even. The address must be a unique unicast MAC address.</p> <p> Tip We recommend that you make a note of the MAC Address Prefix for each VPN Broker Domain.</p> <p> Note With version 6.11, the MAC Address Prefix is auto-populated.</p>
Primary VPN Broker Server	In a high availability environment, one NGFW Manager must be set as the primary NGFW Manager for each VPN Broker Domain. When you make changes to the list of VPN Broker members in the primary NGFW Manager, the changes are synchronized to the other instances of the NGFW Manager. If this NGFW Manager is offline, you must manually promote another NGFW Manager to be the primary.
Enabled	When selected, the VPN Broker Domain element is enabled. You can temporarily disable the element without deleting it.

Next steps

In each NGFW Manager, create one VPN Broker Gateway element to represent the local VPN Broker gateway.

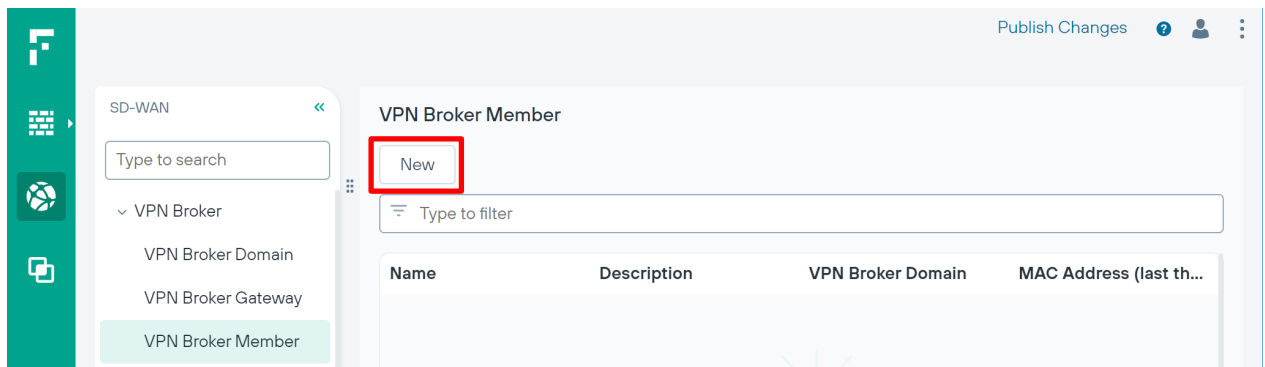
Create VPN Broker Members for VPN Broker high availability

Create VPN Broker Member elements to represent each NGFW Engine that is used in the VPN Broker configuration.

Changes that you make to the list of VPN Broker members in the primary NGFW Manager are automatically synchronized to other gateways.

Steps





- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Member**.



2) Click .

3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

VPN Broker Member properties	
Option	Definition
VPN Broker Domain	Select the VPN Broker Domain element that you created. Type part of the name of an element or browse through the drop-down list to select an element.
Mac Address (last three octets)	<p>Enter a unique identifier for the VPN Broker Member as the last three octets of a MAC address. The allowed range is 00:01:00–ff:ff:ff. Each member in the domain must have a unique identifier. When adding a VPN Broker Interface to an NGFW Engine in the SMC, use the same value that is used in the corresponding VPN Broker Member element in the NGFW Manager.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-bottom: 5px;"> <p> Note</p> <p>The range 00:00:01– 00:00:FF is reserved for the VPN Broker Gateway element. You cannot use identifiers in this range for members in the domain.</p> </div> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-bottom: 5px;"> <p> Tip</p> <p>We recommend that you make a note of the MAC addresses for each VPN Broker Member.</p> </div> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> Note</p> <p>With version 6.11, the MAC Address (last three octets) is auto-populated.</p> </div>
Shared Secret	<p>Click Enter Shared Secret to enter a password. Click Change Shared Secret to change a password that has already been set.</p> <p>When adding a VPN Broker Interface to an NGFW Engine in the SMC, use the same value that is used in the corresponding VPN Broker Member element in the NGFW Manager.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px;"> <p> Tip</p> <p>We recommend that you make a note of the shared secret.</p> </div>

Option	Definition
IPv4 Address or IPv6 Address	<p>Enter a member IP address that is part of the virtual network defined in the VPN Broker Domain element. You must enter an IPv4 address, an IPv6 address, or both.</p> <p>Use the same kind of IP address that the VPN Broker Domain uses. For example, if the VPN Broker Domain has only IPv4 addresses, enter an IPv4 address. You can enter both an IPv4 address and an IPv6 address if the VPN Broker Domain has both IPv4 addresses and IPv6 addresses.</p> <div data-bbox="451 415 492 468" style="display: inline-block; vertical-align: middle;"> </div> <div data-bbox="540 422 1469 541" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Tip</p> <p>We recommend that you make a note of the IP addresses for each VPN Broker Member.</p> </div> <div data-bbox="451 579 508 632" style="display: inline-block; vertical-align: middle; margin-top: 10px;"> </div> <div data-bbox="540 579 1469 678" style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>Note</p> <p>With version 6.11, IP address validation is done and notified to the administrator.</p> </div>
<p>Networks table To edit the contents of a cell, click the cell.</p> <p>Click <input type="button" value="New"/> to add the first row. Click ⋮ > New Row Before or ⋮ > New Row After to add a row.</p>	
Network	<p>Select the networks that are reachable through the VPN Broker member. Type part of the name of an element or browse through the drop-down list to select an element.</p>
Mode	<p>Select from the following options.</p> <ul style="list-style-type: none"> ■ Reserved — Network addresses are dedicated to the gateway and these addresses or a subnet of these addresses cannot be given to any other member of the VPN Broker domain. This is the recommended option. ■ Allowed — Network addresses are allowed for the VPN gateway. However, the VPN Broker does not announce these as routes to other VPN gateways. Used for dynamic routing or the default VPN gateway. ■ Routed — When selected, enter a value in the Metric field. The same network address that has a different route metric value can be given to another VPN gateway. The subnet of a specified network can be given to a specified VPN gateway.

Next steps

In the primary NGFW Manager, export the VPN Broker Domain element to a file.

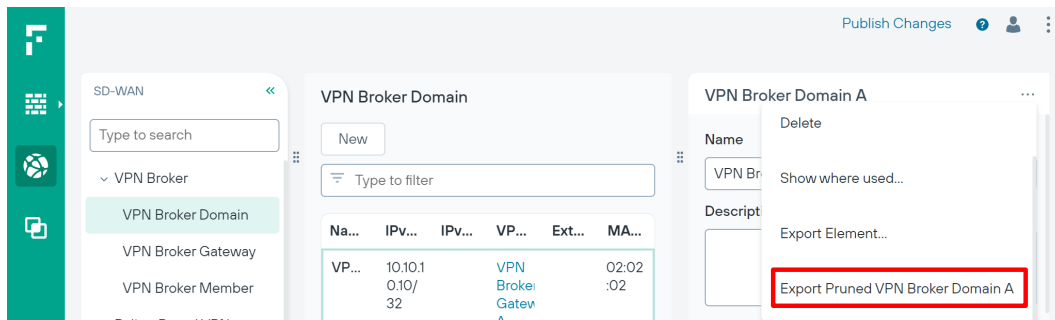
Export a VPN Broker Domain element to a file for high availability

In the primary NGFW Manager, export the VPN Broker Domain element to a file.

The configuration of the VPN Broker Domain element must contain information about all VPN Broker gateways and VPN Broker members in the same VPN Broker domain.

Steps

- 1) Browse to **SD-WAN > VPN Broker > VPN Broker Domain**.



- 2) Select the VPN Broker Domain element that you want to export, then click **:** > **Export Pruned <name>**.
The **Export Pruned** option exports only the parts of the VPN Broker Domain configuration that are needed for creating a VPN Broker Domain element in the SMC. The exported configuration includes the VPN Broker Domain and the VPN Broker Members.
- 3) Save the .zip file to your local workstation.

Next steps

In each NGFW Manager, enable the VPN configuration in the properties of the NGFW Engine.

Enable the VPN configuration in each NGFW Manager

In each NGFW Manager, enable the VPN configuration in the properties of the NGFW Engine.


Steps

- 1) Browse to **NGFW > Properties**.
- 2) Browse to the **VPN** section, then enable **VPN Configuration**.
- 3) To add a row to the **VPN Gateways** table, click **New**.
- 4) In the **VPN Gateway** cell, add the VPN Broker Gateway element that you created.
Type part of the name of an element or browse through the drop-down list to select an element.
- 5) Under **VPN Gateway Settings**, add the Gateway Default Settings element.
Type part of the name of an element or browse through the drop-down list to select an element.
- 6) Click **Save**.

- 7) If you have not yet viewed or edited the Access policy, at the top-right corner of the user interface click: [Finalize the setup](#)

- 8) To publish your changes in the NGFW Manager, at the top-right corner of the user interface, click: [Publish Changes](#)

Fields marked with an asterisk * in the user interface are mandatory.

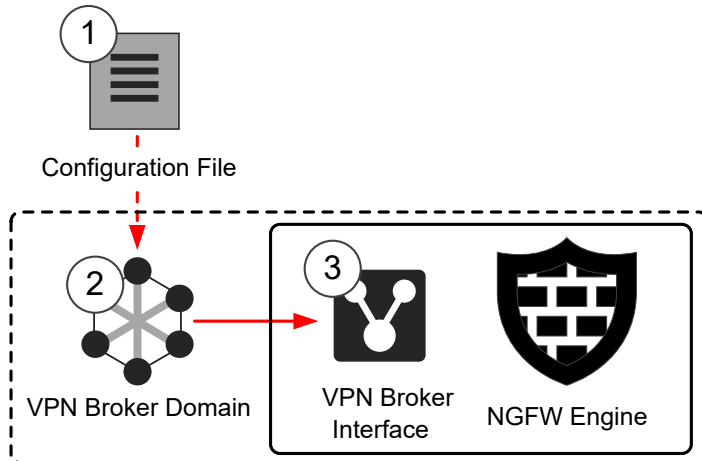
NGFW Engine Properties - VPN	
Option	Definition
VPN Configuration	When enabled, shows the VPN options.
VPN Gateways table	Shows the configured VPN gateways. To edit the contents of a cell, click the cell. Click  to add the first row. Click *** > New Row Before or *** > New Row After to add a row.
Gateway	The VPN Gateway element that represents the physical gateway device. Type part of the name of an element or browse through the drop-down list to select an element.
VPN Client Settings	This option is not yet supported.
SSL VPN Settings	This option is not yet supported.
Automatic Certificate Management	This option is not yet supported.
Automatic Sites From Routing	This option is not yet supported.
VPN Gateway Settings	The VPN Gateway Settings element defines performance-related VPN options. Type part of the name of an element or browse through the drop-down list to select an element.

Next steps

You have now finished the configuration steps in the NGFW Manager. Next, create elements for the VPN Broker high availability configuration in the SMC.

Create elements for the VPN Broker high availability configuration in the SMC

You must create the elements that represent the VPN Broker configuration in the SMC.



- 1 The configuration file for the VPN Broker Domain is exported from the NGFW Manager.
- 2 The configuration file that you exported from the NGFW Manager is used in the VPN Broker Domain element.
- 3 The VPN Broker Interface is a virtual interface in the configuration of the NGFW Engine. The VPN Broker interface allows the NGFW Engine to act as a member of the VPN Broker domain.

Next steps

Begin by creating a VPN Broker Domain element in the SMC.

Create one VPN Broker Domain element in the SMC

Create one VPN Broker Domain element and import the exported configuration file from the NGFW Manager.

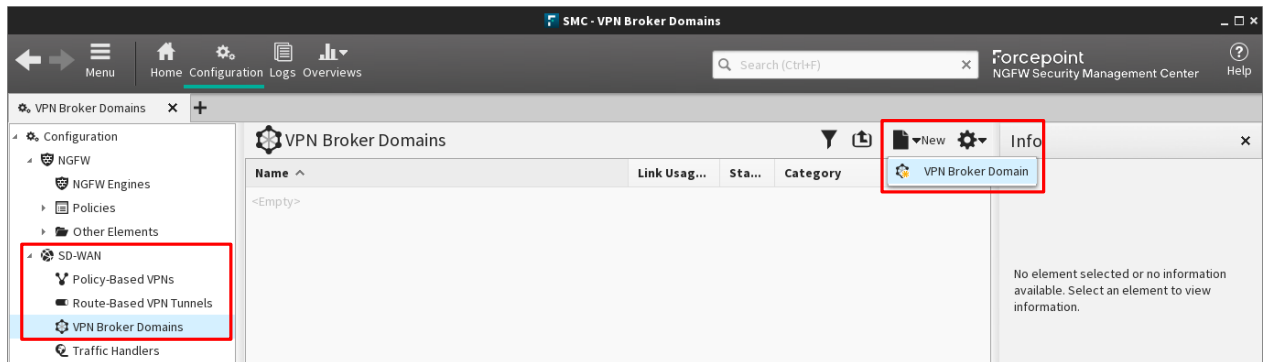


Note

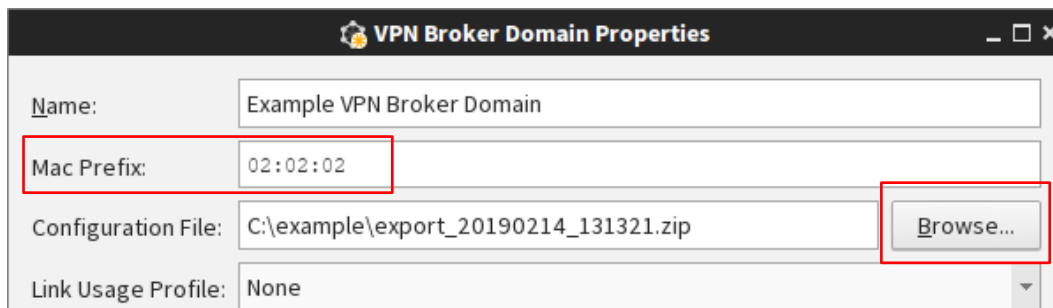
The configuration of the VPN Broker Domain element must contain information about all VPN Broker gateways and VPN Broker members in the same VPN Broker domain.

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

- 1) Open the Management Client.



- 2) Select **Configuration**, then browse to **SD-WAN**.
- 3) Browse to **VPN Broker Domains**.
- 4) Select **New > VPN Broker Domain**.



- 5) Configure the settings.
 - a) (Optional) Enter a name for the element.
If you do not enter a name, the name is automatically generated based on the name of the configuration file.
 - b) In the **Mac Prefix** field, enter the first three octets of the MAC address that is used by all members of the VPN Broker domain.
This MAC address prefix must be the same as the MAC address prefix that is used in the VPN Broker Domain element that you created in the NGFW Manager.
 - c) Next to the **Configuration File** field, click **Browse**, then select the configuration file that you exported from the NGFW Manager.
 - d) Click **OK**.


VPN Broker Domain properties	
Option	Definition
Name (Optional)	The name of the element.
Mac Prefix	Enter the first three octets of the MAC address that is used by all members of the VPN Broker domain. This MAC address prefix must be the same as the MAC address prefix that is used in the VPN Broker Domain element that you created in the NGFW Manager.
Configuration File	Click Browse to select the configuration file that you exported from the NGFW Manager.
Link Usage Profile (Optional)	To use dynamic link selection for Multi-Link VPNs, select a Link Usage Profile element. When you select a Link Usage Profile element in the properties of a policy-based VPN, route-based VPN tunnel group, or a VPN broker domain, the settings defined in the Link Usage Profile element are applied to all tunnels in the VPN according to their link types.

Next steps

Add a VPN Broker Interface to all NGFW Engines that are used as VPN Broker members.

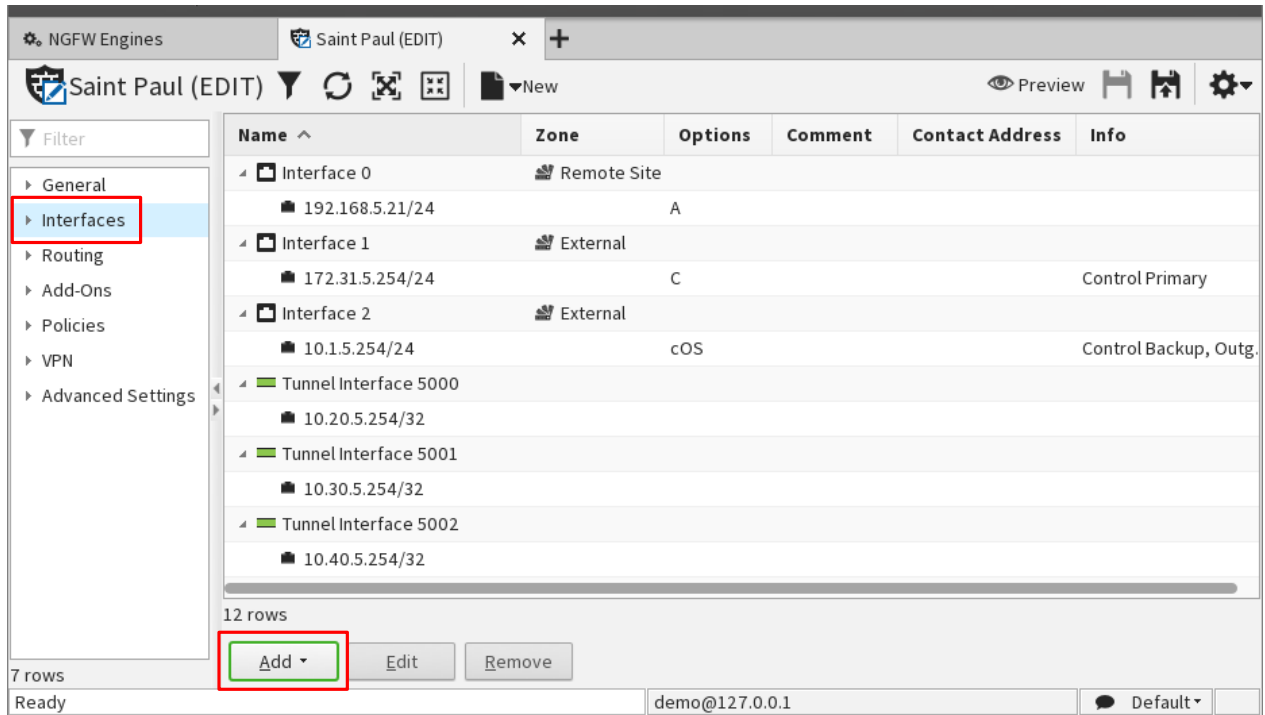
Add a VPN Broker Interface to each NGFW Engine

You must add a VPN Broker Interface to each NGFW Engine that is used as a VPN Broker member so that the VPN Broker can communicate with the members of a VPN Broker domain.

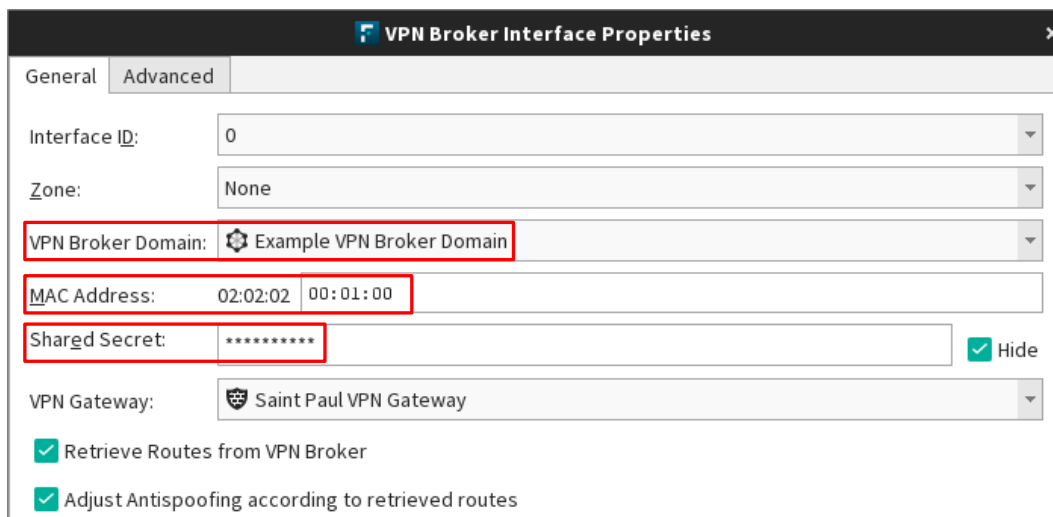
Steps  For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) In the Management Client, select  **Configuration**.

- 2) Right-click an NGFW Engine, then select **Edit <element type>**.



- 3) Browse to **Interfaces**.
- 4) Click **Add > VPN Broker Interface**.
- 5) Configure the settings.



- a) From the **VPN Broker Domain** drop-down list, select the VPN Broker Domain element that you created.
- b) In the **MAC Address** field, enter the last three octets of the MAC address for the VPN Broker member. This MAC address must be the same as the MAC address used in the corresponding VPN Broker Member element that you created in the NGFW Manager.

- c) In the **Shared Secret** field, enter the same password that you entered for the VPN Broker Member element in the NGFW Manager.
 - d) Click **OK**.
- 6) Right-click the VPN Broker Interface, then select **New > IPv4 Address** or **New > IPv6 Address**.
 - 7) Enter the IP address used in the corresponding VPN Broker Member element, then click **OK**.
 - 8) Click **Save and Refresh**, then click **OK** to transfer the changes to the NGFW Engine.

VPN Broker Interface properties	
Option	Definition
General tab	
Interface ID	The ID number that identifies the VPN Broker Interface. The VPN Broker Interface is a virtual interface that is used only for the VPN Broker. The interface ID of the VPN Broker Interface can be the same as the interface ID of a physical interface on the same NGFW Engine.
Zone (Optional)	Select the network zone to which the interface belongs. Click Select to select an element, or click New to create an element.
VPN Broker Domain	Select the VPN Broker Domain element that you created.
MAC Address	<div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-bottom: 10px;"> <p>Note</p> <p>The MAC address prefix for the VPN Broker Domain is automatically added based on the VPN Broker Domain element.</p> </div> <p>Enter the last three octets of the MAC address for the VPN Broker member. This MAC address must be the same as the MAC address used in the corresponding VPN Broker Member element that you created in the NGFW Manager.</p>
Shared Secret	Enter the password. The password must be the same as the shared secret that you entered for the VPN Broker Member element in the NGFW Manager. By default, passwords and keys are not shown in plain text. To show the password or key, deselect the Hide option.
VPN Gateway	Select the local VPN gateway.
Retrieve Routes from VPN Broker	When selected, the routing table is updated with routes that are retrieved by the VPN Broker.
Adjust Antispoofing according to retrieved routes	When selected, antispoofing rules are automatically adjusted based on the routes that are retrieved by the VPN Broker.
QoS Mode (Optional)	Defines how QoS is applied to the link on this interface. If Full QoS or DSCP Handling and Throttling is selected, a QoS policy must also be selected. If Full QoS is selected, the throughput must also be defined. If the interface is a Physical Interface, the same QoS mode is automatically applied to any VLANs created under it.

Option	Definition
<p>QoS Policy</p>	<p><i>(When QoS Mode is Full QoS or DSCP Handling and Throttling)</i></p> <p>The QoS policy for the link on this interface.</p> <p>If the interface is a Physical Interface, the same QoS policy is automatically selected for any VLANs created under it.</p> <div data-bbox="451 373 506 426" style="float: left; margin-right: 10px;"> </div> <div data-bbox="537 373 1468 531" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>If a Virtual Resource has a throughput limit defined, the interfaces on the Virtual NGFW Engine that use a QoS policy all use the same policy. The policy used in the first interface is used for all the interfaces.</p> </div>
<p>Interface Throughput Limit</p>	<p><i>(When QoS Mode is Full QoS)</i></p> <p>Enter the throughput for the link on this interface as megabits per second.</p> <p>If the interface is a Physical Interface, the same throughput is automatically applied to any VLANs created under it.</p> <p>The throughput is for uplink speed (outgoing traffic) and typically must correspond to the speed of an Internet link (such as an ADSL line), or the combined speeds of several such links when connected to a single interface.</p> <div data-bbox="451 846 506 898" style="float: left; margin-right: 10px;"> </div> <div data-bbox="537 846 1468 1031" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>CAUTION</p> <p>Make sure that you set the interface speed correctly. When the bandwidth is set, the NGFW Engine always scales the total amount of traffic on this interface to the bandwidth you defined. This scaling happens even if there are no bandwidth limits or guarantees defined for any traffic.</p> </div> <div data-bbox="451 1066 506 1119" style="float: left; margin-right: 10px;"> </div> <div data-bbox="537 1066 1468 1251" style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>CAUTION</p> <p>The throughput for a Physical Interface for a Virtual NGFW Engine must not be higher than the throughput for the Master NGFW Engine interface that hosts the Virtual NGFW Engine. Contact the administrator of the Master NGFW Engine before changing this setting.</p> </div>
<p>MTU (Optional)</p>	<p>The maximum transmission unit (MTU) size on the connected link. Either enter a value between 400–65535 or select a common MTU value from the list.</p> <p>If the interface is a Physical Interface, the same MTU is automatically applied to any VLANs created under it.</p> <p>The default value (also the maximum standard MTU in Ethernet) is 1500. Do not set a value larger than the standard MTU, unless you know that all devices along the communication path support it.</p> <p>To set the MTU for a Virtual NGFW Engine, you must configure the MTU for the interface on the Master NGFW Engine that hosts the Virtual NGFW Engine, then refresh the policy on the Master NGFW Engine and the Virtual NGFW Engine.</p>

Next steps

Check the status of the VPN Broker.

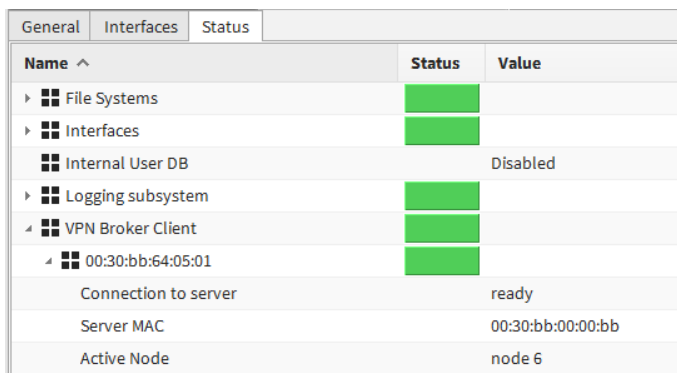
Check the status of the VPN Broker

To make sure that the components in the VPN Broker configuration are working correctly, check the status of the VPN Broker in the Management Client component of the SMC or on the command line of the NGFW Engine.

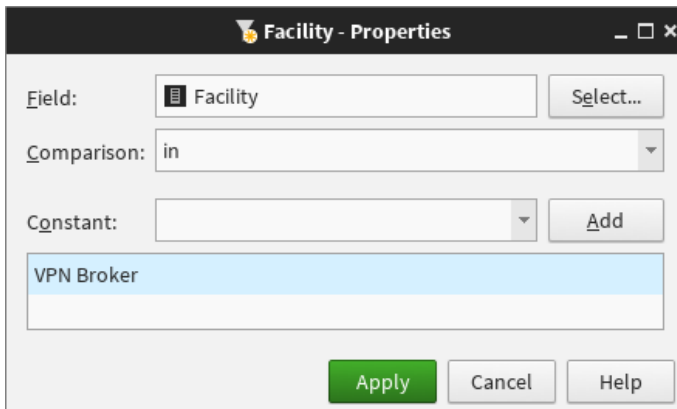
For more information about the monitoring features in the Management Client, see the *Forcepoint Next Generation Firewall Product Guide*.

Steps

- 1) Check the status in one or more of the following ways:
 - In the Home view of the Management Client, select an NGFW Engine to check the status of the connection between the NGFW Engine and the VPN Broker gateway. The **Status** tab of the **Info** pane shows the status.



- In the Logs view of the Management Client, use the VPN Broker facility in a filter to show logs related to the VPN Broker.



The following situations appear in log entries related to the VPN Broker:

Situation	Description
VPN-Broker_Client-Request	A VPN Broker member sent an information request to a VPN Broker gateway.
VPN-Broker_Connection_Error	The connection with the VPN Broker gateway has not been established.
VPN-Broker_Connection_Established	The connection with the VPN Broker gateway has been established.

- When VPN tunnels have been established between VPN Broker members, check the status of the tunnels in the SD-WAN dashboard in the Home view of the Management Client.

- On the command line of an NGFW Engine, enter the following command:

```
sg-brokerctl -s
```

On an NGFW Engine that acts as a VPN Broker gateway, the command shows a summary of the status of the connections between the VPN Broker members and the VPN Broker gateway. In a high availability environment, you can see if the VPN Broker gateways can be contacted. The age shown in the output should be 5 seconds or less. To check that the members have been synchronized correctly, you can enter `sg-brokerctl info` to check that the hash for `primary_member_hash` and `member_hash` match.

On an NGFW Engine that acts as a VPN Broker member, the command shows which other VPN Broker members the NGFW Engine can connect to, and shows the status of the connection between the NGFW Engine and the VPN Broker gateway.

Result

You have now finished configuring the VPN Broker.

Part III

Local management of a single NGFW Engine

Contents

- [Setting up the NGFW Engine for local management on page 81](#)
- [Monitoring the NGFW Engine on page 103](#)
- [Configuring other NGFW Engine properties on page 109](#)

You can use the Forcepoint NGFW Manager to locally manage a single NGFW Engine.

Chapter 4

Setting up the NGFW Engine for local management

Contents

- Example deployment scenario for a single NGFW Engine on page 81
- Limitations of local management of single NGFW Engines on page 82
- NGFW Engine configuration overview on page 82
- Start the NGFW Manager on page 83
- Select the mode in the NGFW Manager on page 84
- Create elements to use for NGFW Engine configuration on page 85
- Configure interfaces for connections to other networks on page 86
- Edit the Access policy on page 90
- Edit the NAT policy on page 94
- Select the Inspection policy for the NGFW Engine on page 96
- Configure SSH access to the NGFW Engine command line on page 96
- Configure NTP on page 97
- Configure DNS on page 98
- Change the IP address of the interface for control connections on page 99
- Create other elements for NGFW Engine configuration on page 100

To use the NGFW Manager for local management of a single NGFW Engine, configure the necessary settings for the NGFW Engine.

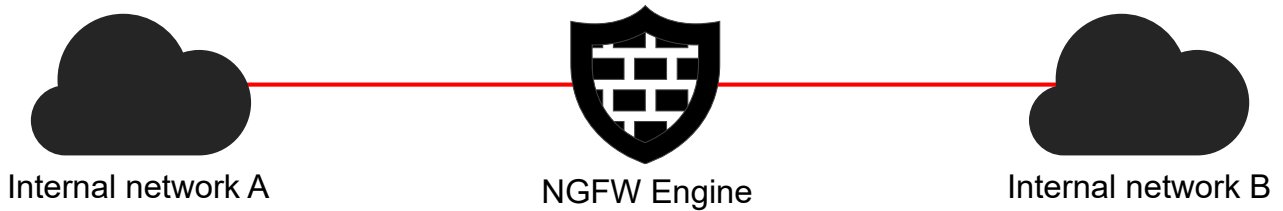


Note

It is not possible to use local management for NGFW Engines that are used as VPN Broker members. You must configure and manage NGFW Engines that are used as VPN Broker members using the Management Client component of the SMC.

Example deployment scenario for a single NGFW Engine

The NGFW Engine is a perimeter defense, positioned between networks with different security levels. This scenario shows an example of using the NGFW Engine to restrict traffic between different internal networks in an isolated network environment.



The NGFW Engine separates the different internal networks by enforcing rules that control access from one network to another. The NGFW Engine establishes boundaries between networks to protect sensitive data and essential services.

Limitations of local management of single NGFW Engines

The NGFW Manager has some restrictions and limitations.



Note

This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

Some features require Internet connectivity.

The following configuration options and features are not yet available in this release:

- Antivirus and McAfee GTI scans for file filtering
- Log forwarding
- Policy routing
- ThreatSeeker Cloud URL categorization
- TLS inspection
- Tunnel interfaces

VPNs are not yet supported in NGFW Engine Management mode. To use the VPN Broker, you must use VPN Broker Management mode.

NGFW Engine configuration overview

The NGFW Engine configuration consists of several general steps.

- 1) Configure interfaces and routing.
 - a) Create elements to use for interface configuration.
 - b) Add IP addresses to interfaces for connections to other networks.
 - c) For networks that are not directly connected to the NGFW Engine, configure routing.

- 2) Configure policies.
 - a) Add rules to the Access policy.
 - b) (Optional) Select the Inspection policy for the NGFW Engine.
- 3) (Optional) To allow secure remote connections to the command line of the NGFW Engine, configure SSH access.
- 4) (Optional) To enable automatic time synchronization for the NGFW Engine, configure NTP.

**Note**

This feature requires Internet connectivity.

- 5) (Optional) To allow the NGFW Engine to translate domain names to IP addresses, configure DNS.

**Note**

This feature requires Internet connectivity.

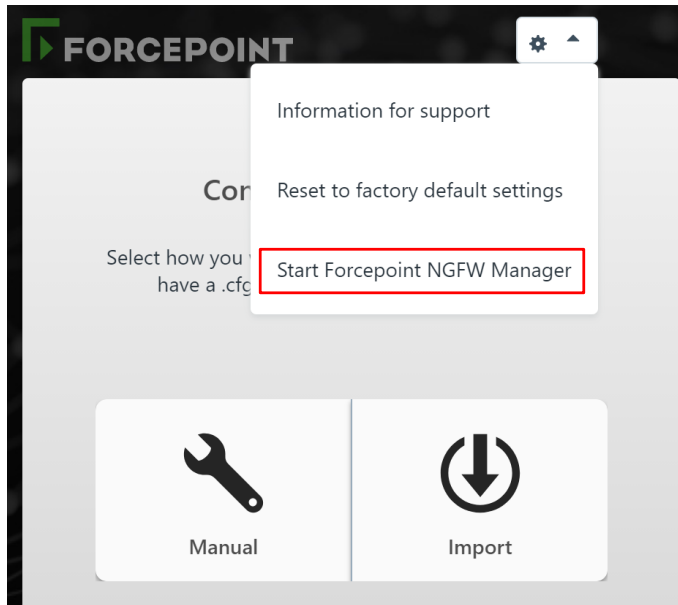
Start the NGFW Manager

The NGFW Configuration Wizard allows you to configure settings for the Forcepoint NGFW appliance. Start the NGFW Manager from the web browser version of the NGFW Configuration Wizard.

Steps

- 1) Connect the NGFW appliance to a laptop or other client device.
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) Connect the other network cables to the Forcepoint NGFW appliance.
- 3) Turn on the Forcepoint NGFW appliance.
- 4) To start the web browser version of the NGFW Configuration Wizard, open a web browser on the client device, then connect to `https://169.254.169.169`.
It might take some time for the web page to load.
- 5) When the NGFW Configuration Wizard offers a web browser client certificate, accept the certificate.
- 6) On the Welcome page of the NGFW Configuration Wizard, click **Start**.
- 7) Select **I Agree to the Terms and Conditions**, then click **Next**.

- 8) Enter and confirm the password for the root account, then click **Next**.



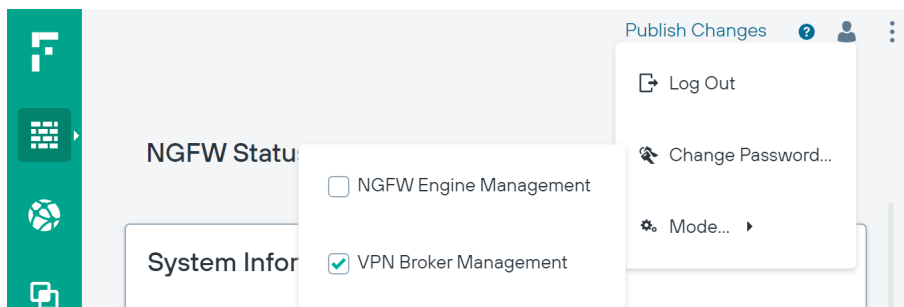
- 9) Click **⚙️ > Start Forcepoint NGFW Manager** to restart the appliance.
- 10) After the NGFW appliance has restarted, refresh the web browser to start the NGFW Manager.
- 11) Enter `root` as the user name, enter the password for the root account, then click **Log In**.

Next steps

Continue by selecting the mode in the NGFW Manager.

Select the mode in the NGFW Manager

Modes in the NGFW Manager allow you to either configure the VPN Broker or locally manage a single NGFW Engine.



Steps

- 1) Select **User > ⚙️ Mode**, then select the mode.

- **VPN Broker Management** — Allows you to configure the VPN Broker. In this mode, elements and options related to the VPN Broker are shown in addition to elements and options related to the management of the NGFW Engine.
- **NGFW Engine Management** — Allows you to locally manage a single NGFW Engine. In this mode, elements and options related to the VPN Broker are not shown.



Note

If you are in the **VPN Broker** branch of the **SD-WAN** view, you cannot change the mode to **NGFW Engine Management**. Browse to a different view, then change the mode.

Next steps

Continue the configuration in one of the following ways:

- If you are configuring the VPN Broker, configure an interface for members of the VPN Broker domain.
- If you are locally managing a single NGFW Engine, create elements to use for NGFW Engine configuration.

Create elements to use for NGFW Engine configuration

Create reusable elements to use in the configuration of the NGFW Engine.

To configure interfaces and routing to networks that are not directly connected to the NGFW Engine, create a Router element to represent your network switch or router, and Network elements to represent the other networks.

To configure SSH access to the command line of the NGFW Engine, create Host or Network elements to define the IP addresses from which SSH connections to the NGFW Engine are allowed.

Steps

- 1) Browse to **Elements > Network Elements > <element type>**.
- 2) Click .
- 3) Configure the settings, then click **Save**.

Fields marked with an asterisk * in the user interface are mandatory.

Host properties	
Option	Definition
IP List	Enter one IP address for the host. Enter one IP address per row. If you have a list of IP addresses where each IP address is on a separate row, you can copy and paste the list. To remove a row, click × Remove next to the row. To remove all rows, click Clear All .

Network element	
Option	Definition
IPv4 Network	Enter the IPv4 address and netmask in CIDR notation. You must enter either an IPv4 or IPv6 network.
IPv6 Network	Enter the IPv6 address and prefix length in CIDR notation. You must enter either an IPv4 or IPv6 network.
Broadcast	When selected, includes the broadcast address and the network address in the definition. The broadcast address is only used when you use the Network element in the Source and Destination cells in rules.

Router element	
Option	Definition
IP List	Enter one or more IP addresses for the router. Enter one IP address per row. If you have a list of IP addresses where each IP address is on a separate row, you can copy and paste the list. To remove a row, click × Remove next to the row. To remove all rows, click Clear All .

Configure interfaces for connections to other networks

Interfaces for each Ethernet port on the NGFW appliance are automatically included in the interface table. You must add IP addresses and configure routing for connections to other networks.

Before you begin

If the other network is not directly connected to the NGFW Engine, create a Router element to represent your network switch or router and a network element to represent the other network.

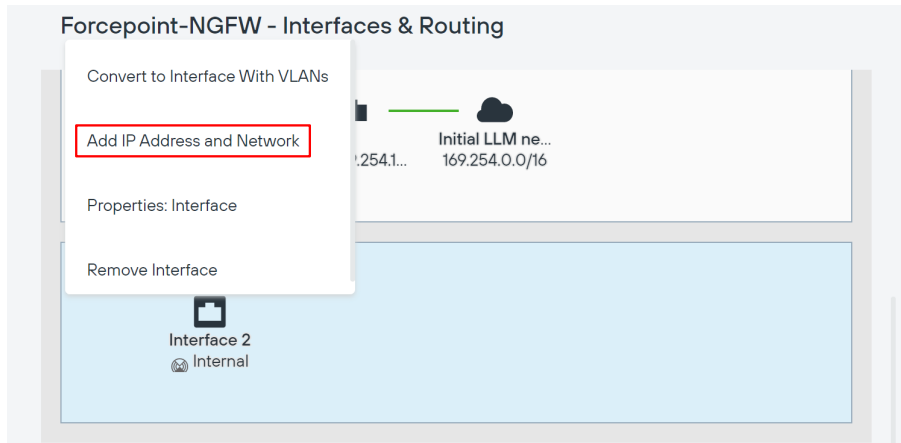


CAUTION

The interface for control connections can only have one IP address. Do not add additional IP addresses or VLANs to the interface for control connections.

Steps

- 1) Browse to **NGFW > Interfaces**.



- 2) In the interface table below the appliance image, click an interface, then select **Add IP Address and Network**.
- 3) Enter the IP address and netmask in CIDR notation, then click **Save**.
Example: 192.168.1.1/24
- 4) If the network is not directly connected to the NGFW Engine, configure routing.
 - a) Click the connected network, select **Add Gateway**, then select your Router element.
 - b) Click the gateway, select **Add Route Target**, then select your Network element.
- 5) Continue the configuration in one of the following ways:
 - If you are configuring interfaces for the first time, click: [Finalize the setup](#)
 - Otherwise, click: [Publish Changes](#)

Fields marked with an asterisk * in the user interface are mandatory.

Interfaces & Routing page	
Option	Definition
<input type="button" value="New"/>	Adds an interface to the interfaces table. If you change the number of Ethernet ports on the NGFW appliance, such as by replacing a 4-port interface module with an 8-port interface module, you must add interfaces to represent the new Ethernet ports. <ul style="list-style-type: none"> ■ Interface — Adds a physical interface. Opens the New Interface pane. ■ Interface with VLANs — Adds a physical interface with a placeholder for adding VLAN interfaces later. Opens the New Interface With VLANs pane. ■ Tunnel Interface — This option is not yet supported.
Appliance image	Shows the ports on the NGFW appliance for which you can configure interfaces. When you select an interface in the interface table, the corresponding port is highlighted in the image.

Option	Definition
Interface table	Allows you to configure the IP addresses, networks, and routing for each interface.
Physical Interface	<p><i>(When interface type is Physical Interface)</i></p> <p>Shows the interface ID of the physical interfaces. The following actions are available when you click the interface:</p> <ul style="list-style-type: none"> ■ Add IP Address and Network — Adds an IP address and a Network element to the interface. Opens the New IP Address and Netmask pane. ■ Convert to Interface With VLANs — Removes any IP addresses that have been specified and converts the interface to an interface with VLANs. ■ Properties: Interface — Opens the interface properties. ■ Remove Interface — Removes the interface from the configuration.
Physical Interface	<p><i>(When interface type is Physical Interface with VLAN interfaces)</i></p> <p>Shows the interface ID of the physical interfaces and the VLAN interfaces under them. The following actions are available when you click the physical interface:</p> <ul style="list-style-type: none"> ■ Add VLAN Interface — Adds a VLAN interface. ■ Convert to Interface — Converts the interface with VLANs to an interface. There can be a maximum of one VLAN Interface when you convert the interface. ■ Properties: Interface with VLANs — Opens the interface properties. ■ Remove Interface — Removes the interface from the configuration. <p>The following actions are available when you click the VLAN interface:</p> <ul style="list-style-type: none"> ■ Add IP Address and Network — Adds an IP address and a Network element to the interface. Opens the New IP Address and Netmask pane. ■ Properties: VLAN Interface — Opens the VLAN interface properties. ■ Remove VLAN Interface — Removes the VLAN interface.
IP Address	<p>Shows the IP address of the physical interface or VLAN interface. The following actions are available when you click the IP address:</p> <ul style="list-style-type: none"> ■ Properties: Static Address — Allows you to add a static IP address to the interface. ■ Remove IP Address and Network — Removes the IP address from the interface configuration.
Connected Network	<p>Shows the network range of the directly connected network. The following options are available when you click the network:</p> <ul style="list-style-type: none"> ■ Add Gateway — Allows you to add a route through a gateway device to a network that is not directly connected. ■ Properties: Network — Opens the properties of the Network element.
Gateway	<p>Shows the gateway device through which the NGFW Engine connects to a network that is not directly connected. The following actions are available when you click the gateway:</p> <ul style="list-style-type: none"> ■ Add Route Target — Allows you to specify the IP addresses that are reachable through the gateway device. ■ Properties: <element type> — Opens the properties of the element that represents the gateway device. ■ Remove Gateway — Removes the gateway device from the interface configuration. The element is not deleted.

Option	Definition
Route Target	Shows the IP addresses that are reachable through the gateway device. The following options are available when you click the route target: <ul style="list-style-type: none"> ■ Properties: <element type> — Opens the properties of the element that represents the IP addresses. ■ Remove Route Target — Removes the route target from the interface configuration. The element is not deleted.

Interface properties

Option	Definition
Interface ID	<i>(When interface type is Physical Interface)</i> The Interface ID automatically maps to a physical network port on the appliance.
VLAN ID	<i>(When interface type is VLAN Interface)</i> Specifies the VLAN ID (1–4094). The VLAN IDs must be the same as the VLAN IDs that are used in the switch at the other end of the VLAN trunk. Each VLAN Interface is identified as Interface-ID.VLAN-ID, for example, 2.100 for Interface ID 2 and VLAN ID 100.
Interface Options (Optional)	Advanced options for interface configuration.
MTU	The maximum transmission unit (MTU) size on the connected link. Enter a value between 576–65000.
Zone	The network zone to which the interface belongs. By default, Interface 0 belongs to the external zone. All other interfaces belong to the internal zone.
Log Compression Override	When selected, the log compression settings defined for the interface override the default log compression settings defined for the NGFW Engine. <ul style="list-style-type: none"> ■ Compress Discard Logs — When selected, enables log compression for discard log entries. ■ Compress Antispoofing Logs — When selected, enables log compression for antispoofing log entries.
Log Rate	The maximum sustained number of log entries per second. The default value is 100 log entries per second.
Log Burst Size	The maximum number of log entries in a single burst. The default value is 1000 log entries.
Antispoofing Elements	This option is not yet supported.
Route Replies Back	This option is not yet supported.

Next steps

If you are configuring the NGFW Engine for the first time, configure the policy for the NGFW Engine.

Related tasks

Configure log handling settings for the NGFW Engine on page 114

Edit the Access policy

The Access policy defines which connections are allowed.

By default, the Access policy contains one rule for testing connectivity that allows HTTP, HTTPS, and ping traffic from all interfaces that belong to the internal zone to any destination. Log entries related to this traffic are stored on the NGFW Engine.

You can edit this rule and add other rules. By default, the NGFW Engine blocks all connections that have not been specifically allowed in the Access policy.

Default rule in the Access policy

Name	Source	Destination	Service	Logging	Action
Connectivity Testing	Internal Zone	ANY	HTTP, HTTPS, Ping	Stored	Allow

Steps

- 1) Browse to **NGFW > Policy > Access** or **NGFW > Policy > NAT**.
- 2) Add a rule in one of the following ways:
 - Click **+ Add First Rule**.
 - Click a rule, select **⋮ > New**, then select **Rule Before** or **Rule After**.
- 3) Configure the settings, then click **Save**.
- 4) Publish the changes.

Fields marked with an asterisk ***** in the user interface are mandatory.

Access Policy	
Option	Definition
Source and Destination	A set of matching criteria that defines the IP addresses and interfaces that the rule matches. <ul style="list-style-type: none"> ■ Type part of the name of an element or browse through the drop-down list to select an element. ■ Click Set to ANY to match any element.
Service	A set of matching criteria that matches traffic based on the Network Application, or protocol and port. <ul style="list-style-type: none"> ■ Type part of the name of an element or browse through the drop-down list to select an element. ■ Click Set to ANY to match any element.

Option	Definition
Logging	<p>Defines logging options for the rule.</p> <ul style="list-style-type: none"> ■ Logging — When selected, enables logging for the rule. ■ Log Level — Defines the log level for matching connections. <ul style="list-style-type: none"> ■ None — Does not create any log entry ■ Transient — Creates a log entry that is shown on the Logs tab, but is not stored. ■ Stored — Creates a log entry that is stored on the NGFW Engine. ■ Essential — Creates a log entry that is shown on the Logs tab and saved for further use. ■ Alert — Triggers an alert with the severity that you define. ■ Automatic — This option is not supported in the Access policy. ■ Severity — When the Log Level is set to Alert, defines the severity of the alert. ■ Advanced Options — Allows you to define advanced logging options.
Authentication	<p>Defines which users can authenticate and the type of authentication required.</p>
Action	<p>Command for the engine to carry out when a connection matches the rule.</p> <ul style="list-style-type: none"> ■ Allow — Allows connections that match the rule. ■ Discard — Discards connections that match the rule. ■ Continue — Sets default options for traffic matching. The options are used for later rules that match the same criteria unless the later rules override the options. ■ Refuse — Refuses connections that match the rule. ■ Jump — The rule processing jumps to a Sub-Policy to continue processing rules. ■ Use VPN — Connections that match the rule are sent into the specified VPN. ■ Decryption — This option is not yet supported. ■ Advanced Options — Allows you to define advanced action options.

Advanced Logging options


Option	Definition
Log Level	<p>Defines the log level for matching connections.</p>
Severity	<p>When the Log Level is set to Alert, defines the severity of the alert.</p>
Connection Closing	<p>Specifies how log entries are created when connections are closed.</p> <ul style="list-style-type: none"> ■ None — No log entries are created. ■ Normal — Both connection opening and closing are logged, but no information about the volume of traffic is collected. ■ Accounting — Both connection opening and closing are logged and information about the volume of traffic is collected.

Option	Definition
Log Compression	<p>When enabled, generated entries are not logged and shown separately when the limits defined in the Max Log Rate or Max Burst Size are reached. Instead, the NGFW Engine creates a single log entry that contains information about the total number of the generated log entries. After the single log entry is created, logging returns to normal and all generated entries are logged and shown separately.</p> <p>Log compression settings in access rules override the default log compression settings defined for the interface and the default log compression settings defined for the NGFW Engine.</p> <ul style="list-style-type: none"> ■ NOT SET — Settings inherited from earlier access rules with the Continue action are used. ■ No Compression — Log compression is disabled. ■ Access — Only logs generated by access rules are compressed. ■ Inspection — Logs generated by both access rules and inspection rules are compressed. <p>When log compression is enabled, the following additional options are available:</p> <ul style="list-style-type: none"> ■ Max Log Rate — The maximum sustained number of log entries per second. The default value is 100 log entries per second. ■ Max Burst Size — The maximum number of log entries in a single burst. The default value is 1000 log entries.
Log User	<p>Defines whether information about users is included in the log data.</p> <ul style="list-style-type: none"> ■ Off — Information about users is not included in the log data. ■ Default — Information about users is included in the log data if information about the user is cached for the connection. Otherwise, only the IP address associated with the user at the time the log is created is included in the log data. Access control by user must be enabled. ■ Enforced — Information about users is always included in the log data if information about the user is available in the user database. If information about the user is not cached for the connection, the NGFW Engine resolves the user information from the IP address. Access control by user must be enabled.
Log Application	<p>Defines whether information about Application detection is included in the log data.</p> <ul style="list-style-type: none"> ■ Off — Information about Application detection is not included in the log data. ■ Default — Information about Application detection is included in the log data if the information is available without additional inspection. ■ Enforced — Information about Application detection is always included in the log data if the Application can be identified.
Log URL Category	<p>Defines whether information about URL categorization is included in the log data.</p> <ul style="list-style-type: none"> ■ Off — URL categories are not included in the log data. ■ Default — URL categories are included in the log data for matching traffic when URL Categories are used as matching criteria in the rule. ■ Enforced — URL categories are always included in the log data if the URL category can be identified.

Advanced Action options

Option	Definition
Decryption	This option is not yet supported.
Deep Inspection	<p>Selects traffic that matches this rule for checking against the Inspection Policy.</p> <ul style="list-style-type: none"> ■ On — The feature is enabled. ■ Off — The feature is disabled.
File Filtering	This option is not yet supported.

Option	Definition
Conntrack Mode	<ul style="list-style-type: none"> ■ Off — The feature is disabled. ■ Default — The settings defined in the NGFW Engine properties are used. ■ Loose — Reply packets are allowed as part of the allowed connection without an explicit Access rule. The NGFW Engine allows some connection patterns and address translation operations that are not allowed in Normal mode. ■ Normal — Reply packets are allowed as part of the allowed connection without an explicit Access rule. The NGFW Engine drops ICMP error messages related to connections that are not currently active in connection tracking (unless explicitly allowed by a rule in the policy). A valid, complete TCP handshake is required for TCP traffic. The NGFW Engine checks the traffic direction and the port parameters of UDP traffic. If the Service cell in the rule contains a Service that uses a Protocol Agent, the NGFW Engine also validates TCP and UDP traffic on the application layer. If a protocol violation occurs, the packet that violates the protocol is dropped. ■ Strict — Reply packets are allowed as part of the allowed connection without an explicit Access rule. The NGFW Engine allows only TCP traffic that strictly adheres to the TCP standard as defined in RFC 793. The NGFW Engine also checks the sequence numbers of the packets in pre-connection establishment states and for RST and FIN packets, and drops packets that are out of sequence. If the Service cell in the rule contains a Service that uses a Protocol Agent, the NGFW Engine also validates the traffic on the application layer. If a protocol violation occurs, the packet that violates the protocol is dropped.
Idle Timeout	<p>The timeout (in seconds) after which inactive connections are closed. This timeout concerns only idle connections. Connections are not cut because of timeouts while the hosts are still communicating.</p> <p>If you enter a timeout, this value overrides the setting defined in the NGFW Engine properties.</p>
Sync Connections	This option is not yet supported.
TCP MSS	<p>When selected, TCP MSS is enforced. Headers are not included in the maximum segment size (MSS) value; MSS concerns only the payload of the packet. Usually, network equipment sends packets at the Ethernet-standard maximum transmission unit (MTU) size of 1500 (including both payload and headers).</p> <ul style="list-style-type: none"> ■ Min — If a TCP packet has an MSS value smaller than the minimum you set here, the packet is dropped. The smaller the data content is, the less efficient the communications become due to the fixed-size headers. Limiting the minimum size can help alleviate certain types of network attacks. Typically, the value you enter is not larger than the default minimum TCP Maximum Segment Size (536). ■ Max — If a TCP packet has an MSS value larger than the maximum, the NGFW Engine overwrites the packet's MSS with the maximum value you set here. Setting the maximum MSS size might be necessary to prevent fragmentation. Typically, the value you enter is lower than the standard Ethernet MTU (1500), taking the packet headers that are added to the MSS into account.
Forward Traffic To	Select a Host or Proxy Server element to forward traffic to.
Forced Next Hop Destination	<p>When enabled, allows you define a forced next hop in the routing for traffic that matches the rule.</p> <ul style="list-style-type: none"> ■ NOT SET — Settings inherited from earlier access rules with the Continue action are used. ■ Nexthop Zone — Traffic is routed through the specified zone before being sent to its destination. ■ IP Address — Traffic is routed through the specified IP address before being sent to its destination.

Option	Definition
Zone	<p><i>When Forced Next Hop Destination is Nexthop Zone</i></p> <p>Select the Zone element through which traffic is routed before being sent to its destination. The traffic is sent out through the interface that is associated with the selected Zone element.</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p> Note</p> <p>The Zone element must be used on only one interface.</p> </div>
IPv4 Address	<i>When Forced Next Hop Destination is IP Address</i>
IPv6 Address	Enter the IP address to which traffic is routed. If the rule matches both IPv4 and IPv6 addresses, you can enter both an IPv4 and an IPv6 address.
Bypass NAT	When selected, NAT is not applied to connections that match the rule.

Related tasks

Configure log handling settings for the NGFW Engine on page 114

Edit the NAT policy

The NAT policy defines how network address translation (NAT) is applied to traffic.

The NAT policy does not contain any rules by default.

Steps

- 1) Browse to **NGFW > Policy > NAT**.
- 2) Add a rule in one of the following ways:
 - Click **+ Add First Rule**.
 - Click a rule, select **⋮ > New**, then select **Rule Before** or **Rule After**.
- 3) Configure the settings, then click **Save**.
- 4) Publish the changes.

Fields marked with an asterisk ***** in the user interface are mandatory.

NAT Policy	
Option	Definition
NAT Service	A set of matching criteria that matches traffic based on the protocol and port.

Option	Definition
NAT Source	<p>A set of matching criteria that defines the source IP addresses and interfaces that the rule matches.</p> <ul style="list-style-type: none"> ■ NAT Source — When selected, enables options in the cell. ■ Type part of the name of an element or browse through the drop-down list to select an element. ■ Click Set to ANY to match any element. ■ NAT Proxy ARP — When selected, allows the engine to answer address queries regarding the translated addresses.
NAT Source Translation	<p>Defines the options for NAT source translation.</p> <ul style="list-style-type: none"> ■ NAT Source — When selected, enables the options in the cell. ■ NAT Type <ul style="list-style-type: none"> ■ Static — Source addresses in matching connections are translated using the same number of IP addresses as there are possible original source addresses. Each translated IP address corresponds to one original IP address. ■ Dynamic — Source addresses in matching connections are translated using a smaller pool of IP addresses than there are original source addresses included in the rule. Many hosts can use the same IP address, and the connections are distinguished by allocating a different TCP or UDP port for each connection. ■ NAT IP Address <ul style="list-style-type: none"> ■ Any — This option is not yet supported. ■ IP Address — The original IP address is translated to the specified IP address. ■ Element — The original IP address is translated to the IP address of the selected Network element. ■ Port Range — When selected, specifies the port range for dynamic IP address translation. <ul style="list-style-type: none"> ■ Min — The start of the port range for IP address translation. ■ Max — The end of the port range for IP address translation.
NAT Destination	<p>A set of matching criteria that defines the destination IP addresses and interfaces that the rule matches and defines the options for NAT destination translation.</p> <ul style="list-style-type: none"> ■ NAT Destination — When selected, enables the options in the cell. ■ Type part of the name of an element or browse through the drop-down list to select an element. ■ Click Set to ANY to match any element. ■ NAT IP Address <ul style="list-style-type: none"> ■ Any — This option is not yet supported. ■ IP Address — The original IP address is translated to the specified IP address. ■ Element — The original IP address is translated to the IP address of the selected Network element. ■ Port Range — When selected, specifies the port range for dynamic IP address translation. <ul style="list-style-type: none"> ■ Min — The start of the port range for IP address translation. ■ Max — The end of the port range for IP address translation. ■ NAT Proxy ARP — When selected, allows the engine to answer address queries regarding the translated addresses.

Select the Inspection policy for the NGFW Engine

The Inspection policy defines how the engines look for patterns in traffic allowed by the Access policy and what happens when a certain type of pattern is found.



Note

Creating custom Inspection Policies is an advanced feature. We recommend using one of the default Inspection Policy elements.

Steps

- 1) Browse to **NGFW > Properties > Policies**.
- 2) Click the **Inspection Policy** field, then select an Inspection Policy element.
Type part of the name of an element or browse through the drop-down list to select an element.
- 3) Click **Save**.
- 4) Publish the changes.

Configure SSH access to the NGFW Engine command line

To allow secure remote connections to the command line of the NGFW Engine, configure SSH access.

Before you begin

Create Host or Network elements to define the IP addresses from which SSH connections to the NGFW Engine are allowed.

Steps

- 1) Browse to **NGFW > Properties > General**.
- 2) Select **SSH Server Enabled**.
- 3) Browse to **NGFW > Properties > Policies**.
- 4) In the **Alias Resolving** settings, add a row to the table in one of the following ways:
 - Click **New** to add the first row.

- Click **⋮** > **New Row Before** or **⋮** > **New Row After** to add a row.
- 5) Define the following alias translation:

Alias	Alias Value
\$ Allowed SSH Remote Sources	The Host or Network elements that represent the IP addresses from which SSH connections to the NGFW Engine are allowed.

Type part of the name of an element or browse through the drop-down list to select an element.

- 6) Click **Save**.
- 7) Publish the changes.

Configure NTP

Network time protocol (NTP) servers provide time synchronization for the NGFW Engine.



Note

This feature requires Internet connectivity.

Steps

- 1) Create an NTP Server element.
This element can be found under **Elements > Network Elements > Server**.
- 2) Browse to **NGFW > Properties > General**.
- 3) Click the **NTP Server** field, then select the NTP Server element.
Type part of the name of an element or browse through the drop-down list to select an element.
- 4) Click **Save**.
- 5) Publish the changes.

Fields marked with an asterisk ***** in the user interface are mandatory.

NTP Server element	
Option	Definition
IP List	The IP addresses of the NTP server. You must enter either an IP address or a host name. Enter one IP address per row. If you have a list of IP addresses where each IP address is on a separate row, you can copy and paste the list. To remove a row, click ✕ Remove next to the row. To remove all rows, click Clear All .
Hostname	The host name of the NTP server. You must enter either an IP address or a host name.

Option	Definition
NTP Key Type	<ul style="list-style-type: none"> ■ None — The NTP Server does not use a key. ■ MD5 — The NTP Server uses an MD5 hash. ■ SHA-1 — The NTP Server uses an SHA-1 hash.
Key ID	<p>(When NTP Key Type is MD5 or SHA-1)</p> <p>Specifies a unique identifier for the key. Enter a value between 1—65534.</p>
Key MD5 or Key SHA-1	<p>(When NTP Key Type is MD5 or SHA-1)</p> <p>Specifies the MD5 or SHA-1 hash.</p>

Configure DNS

The NGFW Engine uses domain name system (DNS) servers to resolve domain names to IP addresses.



Note

This feature requires Internet connectivity.

The NGFW Engine needs DNS resolution to contact services that are defined using URLs or domain names, and to resolve fully qualified domain names (FQDNs) used in policies.

There are two ways to define DNS servers:

- You can create reusable DNS Server elements.
- You can add the IP addresses of DNS servers directly to the NGFW Engine properties.

You can add several DNS servers to the NGFW Engine. The NGFW Engine uses the DNS servers in the order that they are listed. If the first DNS server is not available, the NGFW Engine uses the next DNS server in the list.

Steps

- 1) (Optional) Create a DNS Server element.
This element can be found under **Elements > Network Elements > Server**.
- 2) Browse to **NGFW > Properties > General**.
- 3) In the **DNS Servers** field, define the DNS server in one of the following ways:
 - Select > **Element**, then click the **Element** field and select the DNS Server element. Type part of the name of an element or browse through the drop-down list to select an element.
 - Select > **Address**, then enter the IP address of the DNS server.
- 4) Click **Save**.
- 5) Publish the changes.

Fields marked with an asterisk * in the user interface are mandatory.

DNS Server element	
Option	Definition
IP List	The IP addresses of the DNS server. Enter one IP address per row. If you have a list of IP addresses where each IP address is on a separate row, you can copy and paste the list. To remove a row, click × Remove next to the row. To remove all rows, click Clear All .
Time To Live	Defines how long a DNS entry can be cached before querying the DNS server again.
Update Interval	Defines how often the DNS entries can be updated to the DNS server if the link status changes constantly.

Change the IP address of the interface for control connections

By default, the interface for control connections has an IP address and network configured. You can optionally change the IP address.

Before you begin

Decide what IP address to use as the IP address of the interface for control connections, then make a note of the IP address.

The IP address of the interface for control connections has the following restrictions:

- Only Node Dedicated IP addresses (NDIs) are supported.
- Only IPv4 addresses are supported.
- The interface for control connections can only have one IP address.



CAUTION

Do not add additional IP addresses or VLANs to the interface for control connections.

Steps

- 1) Browse to **NGFW > Interfaces**.
- 2) In the interface table below the appliance image, click the interface for control connections, then select **Remove IP Address and Network**.
The interface for control connections is indicated with the text (Control) after the IP address.
- 3) Click the same interface, then select **Add IP Address and Network**.
- 4) Enter the IP address and netmask in CIDR notation, then click **Save**.
Example: 192.168.1.1/24
- 5) Click the IP address, then select **Properties: Static Address**.

- 6) Select **Primary Mgt**, then click **Save**.
- 7) Continue the configuration in one of the following ways:
 - If you are configuring interfaces for the first time, click: [Finalize the setup](#)
 - Otherwise, click: [Publish Changes](#)

When you publish the changes, your connection to the NGFW Manager is interrupted because the IP address to which you are connected is no longer available.

- 8) Log on to the NGFW Manager at the new IP address.
Example: `https://192.168.1.1/#/en/ngfw/status`

Fields marked with an asterisk * in the user interface are mandatory.

Properties: Static Address	
Option	Definition
Is Used in Antispoofing	When selected, the IP address is included in the antispoofing configuration. Keep this option selected.
CVI	This option is not yet supported.
NDI	When selected, the NGFW Engine node has a dedicated IP address. Keep this option selected.
Primary Mgt	When selected, the IP address is used for control connections to the NGFW Manager interface.




Create other elements for NGFW Engine configuration

Configurations are stored as reusable elements. Different element types are provided for different concepts. For most elements, you can enter an optional name and comment to help you identify the elements that you create.

Steps

- 1) Browse to **Elements** > <element category> > <element type>.
- 2) Click .
- 3) Configure the settings, then click **Save**.
- 4) Publish the changes.

Fields marked with an asterisk * in the user interface are mandatory.

Elements tab	
Option	Definition
Network Elements	Represent the IP addresses used in policies and in the NGFW Engine properties.
Policies	The rules for inspecting and handling network traffic.
Network Applications	<p>Provide a way to dynamically identify traffic patterns related to the use of a particular application. Network Applications are used in the Access policy to match traffic.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> Note It is not possible to create new elements of this type.</p> </div>
Services	Represent the network protocols and ports used in policies. Service elements are used in the Access policy and the NAT policy to match traffic.
Situations	<p>Patterns that deep inspection looks for in traffic. Situation elements are used in the Inspection policy.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> Note It is not possible to create new elements of this type.</p> </div>
File Types	<p>Represent different types of files that can be allowed or blocked.</p> <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 5px; margin-top: 10px;"> <p> Note It is not possible to create new elements of this type.</p> </div>
TLS	These elements are not yet supported.
Other Elements	These elements are not yet supported.

Chapter 5

Monitoring the NGFW Engine

Contents

- [Browse log data](#) on page 103
- [Using the NGFW Engine tester](#) on page 104

Log and alert entries provide information about what is going on in your network environment.

Log and alert entries are most often triggered by rules in the Access policy. Other types of rules can also be configured to create log and alert entries.



Note

This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

Browse log data

Copies of the most recent log and alert entries are stored on the NGFW Engine.

Steps

- 1) Browse to **NGFW > Logs**.
Log events are shown in real time as they are created.
- 2) To view earlier log events, scroll up in the table.

Log Events	
Option	Definition
Kind	The type of policy that triggered the log event.
Creation Time	Log entry creation time.
Component ID	The identifier of the creator of the log entry.
Event ID	Event identifier, unique within one sender.
Sender	IP address of the NGFW Engine that sent the log entry.
Information Message	A description of the log event that further explains the entry.
Facility	The NGFW Engine subsystem that generated the log event.
Type	Log entry severity type.
Action	Action of the rule that triggered the log event. The action values are Allow, Discard, Refuse, Terminate, Wait for further actions, and Wait for authentication.
Rule Tag	Rule tag of the rule that triggered the log event.


Option	Definition
Src Addr	Packet source IP address.
Dst Addr	Packet destination IP address.
Src Port	TCP or UDP source port in the packet header.
Dst Port	TCP or UDP destination port in the packet header.
IP Protocol	IP protocol of the traffic that generated the log event.
IP Version	Version field value in the IP header.
Event	The event that triggered the log creation, for example, New connection, Connection closed, Connection discarded.
Situation	The identifier of the situation that triggered the log event.
Syslog	Syslog is a system service used in some operating systems, for example, UNIX, and software packages. For more information about syslog and syslog types, see RFC 3164.
Daemon	The name of the daemon that generated the log event.

Using the NGFW Engine tester

The NGFW Engine tester runs various checks on the NGFW Engine and initiates responses based on the success or failure of these tests.

Enable the NGFW Engine tester and specify global settings

The global settings of the tester have default values that you can override to meet your needs.

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

- 1) Browse to **NGFW > Properties > General**.
- 2) Enable **Tester Parameters**.
- 3) Configure the settings, then click **Save**.
- 4) Publish the changes.

NGFW Engine Properties - General - Tester Parameters

Option	Definition
Tester Parameters	<p>When selected, you can configure the global settings for the NGFW Engine tester.</p> <ul style="list-style-type: none"> ■ Alert Interval — Specify the time in minutes the NGFW Engine waits before sending a new alert when the same test keeps failing repeatedly. The default value is 60 minutes. If the interval is too short, the alerts can overload the system or the alert recipient. ■ Delay After Boot — The time in seconds that the NGFW Engine waits before it resumes running the tests after it starts up. The default is 30 seconds. ■ Delay After Reconfiguration — The time in seconds that the NGFW Engine waits before it resumes running the tests after a configuration change. The default is 5 seconds. ■ Delay After Status Change — The time in seconds that the NGFW Engine waits before it resumes running the tests after the status of the NGFW Engine changes. The default is 5 seconds. ■ Is Auto Recovery — When selected, the NGFW Engine automatically goes back online when a previously failed test completes successfully. Run the test in both online and offline states if you activate this option. ■ Is Boot Recovery — When selected, the NGFW Engine automatically goes back online after restarting if all offline tests report a success.

Add NGFW Engine tests

Add NGFW Engine tests and configure the settings for each test.

Before you begin

Enable the NGFW Engine tester and specify global settings.

The following tests are available:

- **Engine Properties Test External** — Runs a command or custom script stored on the NGFW Engine. If the command or script returns the code zero (0), the test is considered successful, otherwise the test is considered failed.
- **Engine Properties Test File Space** — Checks the free disk space on a hard disk partition.
- **Engine Properties Test Swap Space** — Checks the available swap space on the hard disk.
- **Engine Properties Test Link Status** — Checks whether a network port reports the link as up or down.
- **Engine Properties Test Multiping** — Sends out a series of ping requests to determine whether there is connectivity through a network link.



Note

Engine Properties Test Inline Link is only available for inline interfaces. Inline interfaces are not yet supported on the NGFW Manager.


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

- 1) Browse to **NGFW > Properties > General**.

- 2) In the **Test** cell of the **Tests** table, click , then select the type of test to add.
- 3) Configure the settings, then click **Save**.
- 4) Click **Save**.
- 5) Publish the changes.

NGFW Engine Properties - General - Tests	
Option	Definition
Tests	Shows the configured NGFW Engine tests. To add a row to the list, click <input type="button" value="New"/> .
Active	When selected, the NGFW Engine test is active.
Test	Shows the name of the NGFW Engine test. Add a test in one of the following ways: <ul style="list-style-type: none"> ■ Click <input type="button" value="New"/> , then select the type of test to add. ■ Type part of the name of an element or browse through the drop-down list to select an element.

Engine Properties Test External

Option	Definition
Is Run Online	When selected, the test is run when the NGFW Engine node is online.
Is Run Offline	When selected, the test is run when the NGFW Engine node is offline.
Is Run Standby	This option is only available for clusters. Clusters are not yet supported on the NGFW Manager.
Test Interval	Specify in seconds how frequently the test is run.
Action in Failure	Select the action taken if a test fails. <ul style="list-style-type: none"> ■ None — No action is taken. ■ Offline — This option is only available for clusters. Clusters are not yet supported on the NGFW Manager. ■ Force Offline — The NGFW Engine node goes offline, even if the node is in the Locked Online state. Use in cases in which a complete cut in traffic is a better option than a partially working NGFW Engine.
Is Alert	When selected, sends an alert to notify administrators that a test has failed.
Retry Count	Enter the number of times the tester tries to execute the test.
Timeout	Enter the timeout in seconds. If the test being run does not return a response in the specified time, the test has failed. Avoid overly short timeout values. We recommend a timeout of 500–1000 ms, depending on the test.
Command Line	Enter the command or script path. The result must return an exit code of 0 (zero) if it succeeds. Any non-zero return value is a failure. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  <p>CAUTION</p> <p>This test allows administrators who have permissions to edit the properties of NGFW Engines to run arbitrary commands in the NGFW Engine operating system.</p> </div>
Clear All	Reverts your changes.

Engine Properties Test File Space

Option	Definition
Is Run Online	When selected, the test is run when the NGFW Engine node is online.
Is Run Offline	When selected, the test is run when the NGFW Engine node is offline.
Is Run Standby	This option is only available for clusters. Clusters are not yet supported on the NGFW Manager.
Test Interval	Specify in seconds how frequently the test is run.
Action in Failure	Select the action taken if a test fails. <ul style="list-style-type: none"> ■ None — No action is taken. ■ Offline — This option is only available for clusters. Clusters are not yet supported on the NGFW Manager. ■ Force Offline — The NGFW Engine node goes offline, even if the node is in the Locked Online state. Use in cases in which a complete cut in traffic is a better option than a partially working NGFW Engine.
Is Alert	When selected, sends an alert to notify administrators that a test has failed.
Retry Count	Enter the number of times the tester tries to execute the test.
Partition	Specify the partition to test.
Free Space	Enter the minimum amount of free space in kilobytes. When the amount of free space drops below this amount, the NGFW Engine executes the chosen action.

Engine Properties Test Swap Space

Option	Definition
Is Run Online	When selected, the test is run when the NGFW Engine node is online.
Is Run Offline	When selected, the test is run when the NGFW Engine node is offline.
Is Run Standby	This option is only available for clusters. Clusters are not yet supported on the NGFW Manager.
Test Interval	Specify in seconds how frequently the test is run.
Action in Failure	Select the action taken if a test fails. <ul style="list-style-type: none"> ■ None — No action is taken. ■ Offline — This option is only available for clusters. Clusters are not yet supported on the NGFW Manager. ■ Force Offline — The NGFW Engine node goes offline, even if the node is in the Locked Online state. Use in cases in which a complete cut in traffic is a better option than a partially working NGFW Engine.
Is Alert	When selected, sends an alert to notify administrators that a test has failed.
Retry Count	Enter the number of times the tester tries to execute the test.
Free Swap Space	Enter the minimum amount of free space in kilobytes. When the amount of free space drops below this amount, the NGFW Engine executes the chosen action.

Engine Properties Test Link Status

Option	Definition
Is Run Online	When selected, the test is run when the NGFW Engine node is online.
Is Run Offline	When selected, the test is run when the NGFW Engine node is offline.

Option	Definition
Is Run Standby	This option is only available for clusters. Clusters are not yet supported on the NGFW Manager.
Test Interval	Specify in seconds how frequently the test is run.
Action in Failure	Select the action taken if a test fails. <ul style="list-style-type: none"> ■ None — No action is taken. ■ Offline — This option is only available for clusters. Clusters are not yet supported on the NGFW Manager. ■ Force Offline — The NGFW Engine node goes offline, even if the node is in the Locked Online state. Use in cases in which a complete cut in traffic is a better option than a partially working NGFW Engine.
Is Alert	When selected, sends an alert to notify administrators that a test has failed.
Retry Count	Enter the number of times the tester tries to execute the test.
Link Scope	Select the interface on which the test is run. <ul style="list-style-type: none"> ■ All — All interfaces. ■ All with CVI — This option is only available for clusters. Clusters are not yet supported on the NGFW Manager. ■ Specific — A specific physical interface only.
Physical Interface	(When <i>Link Scope</i> is <i>Specific</i>) Select the physical interface to run the test on.

Engine Properties Test Multiping

Option	Definition
Is Run Online	When selected, the test is run when the NGFW Engine node is online.
Is Run Offline	When selected, the test is run when the NGFW Engine node is offline.
Is Run Standby	This option is only available for clusters. Clusters are not yet supported on the NGFW Manager.
Test Interval	Specify in seconds how frequently the test is run.
Action in Failure	Select the action taken if a test fails. <ul style="list-style-type: none"> ■ None — No action is taken. ■ Offline — This option is only available for clusters. Clusters are not yet supported on the NGFW Manager. ■ Force Offline — The NGFW Engine node goes offline, even if the node is in the Locked Online state. Use in cases in which a complete cut in traffic is a better option than a partially working NGFW Engine.
Is Alert	When selected, sends an alert to notify administrators that a test has failed.
Retry Count	Enter the number of times the tester tries to execute the test.
Clear All	Reverts your changes.
Target Addresses	Enter the IP addresses that you want to ping. Enter one IP address per row. If you have a list of IP addresses where each IP address is on a separate row, you can copy and paste the list. To remove a row, click × Remove next to the row. To remove all rows, click Clear All .
Source Address	Select the IP address to use as the source of the ping.

Chapter 6

Configuring other NGFW Engine properties

Contents

- Configure general settings for the NGFW Engine on page 109
- Configure policy settings for the NGFW Engine on page 111
- Configure VPN settings for the NGFW Engine on page 113
- Configure log handling settings for the NGFW Engine on page 114
- Add-ons for the NGFW Engine on page 115

You can optionally configure other NGFW Engine properties if necessary.



Note

This document describes the currently supported features and options. Some features and options that are not yet supported might appear in the user interface.

Configure general settings for the NGFW Engine

General settings include high-level properties of the NGFW Engine, and settings for NTP and DNS.


Steps

- 1) Browse to **NGFW > Properties > General**.
- 2) Configure the settings, then click **Save**.
- 3) Publish the changes.

Fields marked with an asterisk * in the user interface are mandatory.

NGFW Engine Properties - General

Option	Definition
NTP Server	Specifies the NTP Server element that the NGFW Engine uses.
DNS Servers	Specifies the DNS Server elements or IP addresses of the DNS servers that the NGFW Engine uses. The NGFW Engine uses the DNS servers in the order that they are listed. If the first DNS server is not available, the NGFW Engine uses the next DNS server in the list.

Option	Definition
SSH Server Enabled	When selected, SSH access to the command line of the NGFW Engine is enabled. You must separately specify the IP addresses that are allowed to connect to the NGFW Engine using SSH.
Keyboard Layout	This option is not yet supported.
Timezone	This option is not yet supported.
Main Physical Interface	This option is not yet supported.
Diagnostics	Select from the following: <ul style="list-style-type: none"> ■ Authentication — When selected, authentication diagnostic information is included in log data. ■ IPsec — When selected, IPsec VPN diagnostic information is included in log data. ■ Latency Measurements — When selected, information about latency measurements is included in log data.
Log Forwarder	This option is not yet supported.
Tester Parameters	When selected, you can configure the global settings for the NGFW Engine tester. <ul style="list-style-type: none"> ■ Alert Interval — Specify the time in minutes the NGFW Engine waits before sending a new alert when the same test keeps failing repeatedly. The default value is 60 minutes. If the interval is too short, the alerts can overload the system or the alert recipient. ■ Delay After Boot — The time in seconds that the NGFW Engine waits before it resumes running the tests after it starts up. The default is 30 seconds. ■ Delay After Reconfiguration — The time in seconds that the NGFW Engine waits before it resumes running the tests after a configuration change. The default is 5 seconds. ■ Delay After Status Change — The time in seconds that the NGFW Engine waits before it resumes running the tests after the status of the NGFW Engine changes. The default is 5 seconds. ■ Is Auto Recovery — When selected, the NGFW Engine automatically goes back online when a previously failed test completes successfully. Run the test in both online and offline states if you activate this option. ■ Is Boot Recovery — When selected, the NGFW Engine automatically goes back online after restarting if all offline tests report a success.
Tests	Shows the configured NGFW Engine tests. To add a row to the list, click <input type="button" value="New"/> .
Health Responders	Shows the configured health responders that respond to Amazon Route 53 health checkers. <div style="border: 1px solid #ccc; background-color: #f9f9f9; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>You must configure health checkers in AWS before you configure the settings in the NGFW Manager.</p> </div>
<input type="button" value="New"/>	Adds a health responder of the selected type: <ul style="list-style-type: none"> ■ TCP ■ HTTP <p>Select the same protocol that is configured in AWS.</p>
Listen on IP Addresses	Enter or select the IP address of the health checkers that the NGFW Engine responds to. Entering 0.0.0.0 as the IP address means that the NGFW Engine responds to all health checkers.
Port	Enter the port number used for communication with the health checkers. Enter the same port that is configured in AWS.

Option	Definition
Configuration Version	This option is not yet supported.

Related tasks

Configure NTP on page 97

Configure DNS on page 98

Configure SSH access to the NGFW Engine command line on page 96

Configure policy settings for the NGFW Engine

Policy settings specify which policies the NGFW Engine uses, as well as settings for element-based NAT, alias translation, and automatic rules.

Steps

- 1) Browse to **NGFW > Properties > Policies**.
- 2) Configure the settings, then click **Save**.
- 3) Publish the changes.

Fields marked with an asterisk * in the user interface are mandatory.

NGFW Engine Properties - Policies	
Option	Definition
Layer3 Policy	The selected Layer 3 Policy for the NGFW Engine. We recommend that you do not change this setting.
Inspection Policy	The selected Inspection Policy for the NGFW Engine.
File Filtering Policy	This option is not yet supported.
NAT Definition	When enabled, shows options for element-based NAT.
Alias Resolving	<p>Click <input type="button" value="New"/> to add the first row.</p> <p>Click *** > New Row Before or *** > New Row After to add a row.</p> <ul style="list-style-type: none"> ■ Alias — The Alias element. Type part of the name of an element or browse through the drop-down list to select an element. ■ Alias Value — The translated value of the Alias element. Type part of the name of an element or browse through the drop-down list to select an element.
Automatic Rules Settings	When enabled, shows options for automatic rules.

NGFW Engine Properties - Policies - NAT Definition	
Option	Definition
NAT Element Array	Click *** > Add to add definitions for element-based NAT.
NAT Type	Select the translation type. <ul style="list-style-type: none"> ■ Static — Static network address translation is used. For each original address there is a single, predefined translated address. ■ Dynamic — Dynamic network address translation is used. Dynamic NAT uses ports to track connections using the same IP address.
NAT Address Private	The element that represents the private IP address. Type part of the name of an element or browse through the drop-down list to select an element.
NAT Address Public	Select the source of the public IP address. <ul style="list-style-type: none"> ■ NAT Default — The default address is used as the public IP Address. ■ IP Address — Enter an IP address. ■ NAT Interface Addr — Click +, then select an interface. ■ Element — Type part of the name of an element or browse through the drop-down list to select an element.
NAT Port Filter	To limit NAT only to traffic that goes to selected destination ports, select a Service or Service Group element to act as a port filter. The Service or Service Group element includes the destination port information (a single destination port or a range of ports). Type part of the name of an element or browse through the drop-down list to select an element.
NAT Default Enabled	The NGFW Engine uses the default NAT address as the public IP address if there is not a more specific NAT definition that matches the traffic. When you select this option, a NAT rule is generated at the end of the NAT rules in the policy. If no NAT rule matches the traffic, no NAT is applied unless you enable the Default NAT Address.

NGFW Engine Properties - Policies - Automatic Rules Settings	
Option	Definition
Logging	When enabled, shows the logging options.
Log Level	The log level for traffic that matches automatic rules. <ul style="list-style-type: none"> ■ None — Does not create any log entry ■ Transient — Creates a log entry that is shown on the Logs tab, but is not stored. ■ Stored — Creates a log entry that is stored on the NGFW Engine. ■ Essential — Creates a log entry that is shown on the Logs tab and saved for further use. ■ Alert — Triggers an alert with the severity that you define. ■ Automatic — This option is not supported in the Access policy.
Severity	When the Log Level is set to Alert , defines the severity of the alert.
Connection Closing	Specifies how log entries are created when connections are closed. <ul style="list-style-type: none"> ■ None — No log entries are created. ■ Normal — Both connection opening and closing are logged, but no information about the volume of traffic is collected. ■ Accounting — Both connection opening and closing are logged and information about the volume of traffic is collected.


Option	Definition
Log User	<p>Defines whether information about users is included in the log data.</p> <ul style="list-style-type: none"> ■ Off — Information about users is not included in the log data. ■ Default — Information about users is included in the log data if information about the user is cached for the connection. Otherwise, only the IP address associated with the user at the time the log is created is included in the log data. Access control by user must be enabled. ■ Enforced — Information about users is always included in the log data if information about the user is available in the user database. If information about the user is not cached for the connection, the NGFW Engine resolves the user information from the IP address. Access control by user must be enabled.
Log URL Category	<p>Defines whether information about URL categorization is included in the log data.</p> <ul style="list-style-type: none"> ■ Off — URL categories are not included in the log data. ■ Default — URL categories are included in the log data for matching traffic when URL Categories are used as matching criteria in the rule. ■ Enforced — URL categories are always included in the log data if the URL category can be identified.

Configure VPN settings for the NGFW Engine

VPN settings are not yet supported in NGFW Engine Management mode.

Steps

- 1) Browse to **NGFW > Properties > VPN**.
- 2) Configure the settings, then click **Save**.
- 3) Publish the changes.

NGFW Engine Properties - VPN	
Option	Definition
VPN Configuration	When enabled, shows the VPN options.
VPN Gateways table	<p>Shows the configured VPN gateways.</p> <p>To edit the contents of a cell, click the cell.</p> <p>Click  to add the first row.</p> <p>Click *** > New Row Before or *** > New Row After to add a row.</p>
Gateway	The VPN Gateway element that represents the physical gateway device. Type part of the name of an element or browse through the drop-down list to select an element.
VPN Client Settings	This option is not yet supported.
SSL VPN Settings	This option is not yet supported.

Option	Definition
Automatic Certificate Management	This option is not yet supported.
Automatic Sites From Routing	This option is not yet supported.
VPN Gateway Settings	The VPN Gateway Settings element defines performance-related VPN options. Type part of the name of an element or browse through the drop-down list to select an element.

Configure log handling settings for the NGFW Engine

In the log handling settings, you can configure log compression and define what happens when the log spool on the NGFW Engine becomes full.

Log compression allows you to define the maximum number of separately logged entries. When the defined limit is reached, a single antispooofing log entry or discard log entry is logged. The single log entry contains information about the total number of antispooofing log entries or discard log entries. The individual log entries are deleted. After the single log entry is created, logging returns to normal and all entries are logged and shown separately.

The general log compression settings are applied as default settings on all interfaces. You can also define log compression and override the global settings in the properties of each interface.



Note

Do not enable log compression if you want all antispooofing and discard entries to be logged as separate log entries, such as for reporting or statistics.

Steps

- 1) Browse to **NGFW > Properties > General**.
- 2) Configure the settings, then click **Save**.
- 3) Publish the changes.

Fields marked with an asterisk * in the user interface are mandatory.

NGFW Engine Properties - Log Handling	
Option	Definition
Log Spooling Policy	<p>Defines what happens when the log spool becomes full.</p> <ul style="list-style-type: none"> ■ Stop Traffic — The NGFW Engine stops processing traffic and goes offline. ■ Discard Logs — Log entries are discarded in four stages, according to available space. Monitoring data is discarded first, followed by log entries marked as Transient and Stored, and finally log entries marked as Essential. The NGFW Engine continues to process traffic. <p>To use log compression, you must select the Discard Logs option. When you use log compression, log entries are discarded proactively according to the Log Rate and Log Burst Size settings.</p>

Option	Definition
Log Compression	When enabled, enables log compression for the selected types of log entries. <ul style="list-style-type: none">■ Discard Logs — When enabled, log compression is enabled for discard log entries.■ Antispoofing Logs — When enabled, log compression is enabled for antispoofing log entries. This option is enabled by default when you enable Log Compression.
Log Rate	The maximum sustained number of log entries per second. The default value is 100 log entries per second.
Log Burst Size	The maximum number of log entries in a single burst. The default value is 1000 log entries.

Related tasks

[Configure interfaces for connections to other networks](#) on page 86

[Edit the Access policy](#) on page 90

Add-ons for the NGFW Engine

Add-ons are not yet supported.

Part IV

Maintenance

Contents

- [Maintenance tasks on page 119](#)

Most maintenance tasks can be done for both the VPN Broker and for single NGFW Engines.

Chapter 7

Maintenance tasks

Contents

- Upload, import, and activate dynamic update packages on page 119
- Upgrade a single NGFW Engine on page 120
- Change your password on page 122
- Export elements on page 122
- Import elements on page 123
- Back up system configurations on page 123
- Restore backups on page 124
- Restart the NGFW Engine on page 125
- Turn off the NGFW Engine on page 125
- Collect information for Forcepoint support on page 126
- Reset the NGFW appliance to default settings on page 126

Maintenance includes procedures that you do not typically need to do frequently.

Upload, import, and activate dynamic update packages

The NGFW appliance is delivered with a dynamic update package. You can manually upload, import, and activate new dynamic update packages.

Only one dynamic update package at a time can be active.

Steps

- 1) Go to <https://https://dep-downloads.ngfw.forcepoint.com>.
- 2) On the **LLM Dynamic Updates** tab, download the latest dynamic update package .zip file. For details about the dynamic update package, click **Release Notes** under the .zip file.
- 3) Save the update package file to a location accessible from the computer where you use the NGFW Manager.



Note

Make sure that the checksums for the original files and the files that you have downloaded match.

- In the NGFW Manager, select **NGFW > Status**.

System Information

Hostname

Forcepoint-NGFW

Model

virtual_appliance

Installed Policy

Initial Policy

Update Package


LLM Dynup 1222


[Manage...](#)

Version

6.8.0.24032

[Upgrade...](#)

- In the System Information pane, click **Manage** below the update package information.
- Click  **Upload dynup-file**, browse to the dynamic update file, then click **Open**.
- To import the dynamic update package, click **...** > **Import**.
- To activate the dynamic update package, click **...** > **Activate**.

Manage Update Packages	
Option	Definition
Update Package	Shows the name of the update package.
Creation Date	Shows the date that the update package was created.
State	Shows the status of the dynamic update package.
...	The following actions are available: <ul style="list-style-type: none"> ■ Import — Imports the uploaded dynamic update package. ■ Activate — Activates the imported dynamic update package. ■ Delete — Deletes the selected dynamic update package.
 Upload dynup-file	Click to upload a dynamic update file to the NGFW Engine.

Upgrade a single NGFW Engine

You can upgrade a single NGFW Engine using the NGFW Manager.

Steps

- 1) Go to <https://support.forcepoint.com>.
- 2) Enter your license code or log on using an existing user account.
- 3) Select **Downloads**.
- 4) Under **Network Security**, click the version of the Forcepoint NGFW software that you want to download, then download the .zip file installation file.
- 5) Save the Forcepoint NGFW Engine upgrade file to a location accessible from the where computer you use the NGFW Manager.



Note

Make sure that the checksums for the original files and the files that you have downloaded match.

- 6) In the NGFW Manager, select **NGFW > Status**.

System Information

Hostname

Forcepoint-NGFW

Model

virtual_appliance

Installed Policy

Initial Policy

Update Package

LLM Dynup 1222

[Manage...](#)

Version

6.8.0.24032

[Upgrade...](#)



- 7) In the System Information pane, click **Upgrade** below the version information.
- 8) Click **Upload software upgrade**, browse to the Forcepoint NGFW Engine upgrade file, then click **Open**.
- 9) Click **Upgrade**.

Software Upgrade	
Option	Definition
Upload software upgrade	Click to upload a Forcepoint NGFW Engine upgrade file.
Upgrade	Click to start the upgrade.

Change your password

We recommend that you change your password regularly.

Steps

- 1) Click  **User** >  **Change Password**.
- 2) Enter your current password, then enter and confirm the new password.
- 3) Click **Change Password**.

Export elements

Exporting elements allows you to reuse or restore elements for single NGFW Engine configuration without having to create them again.



When you export elements, you can reuse elements in a different NGFW Manager or restore elements that have been deleted.



Note

Exported files are meant for importing elements into the NGFW Manager. They are not meant to be viewed or edited in external applications.

Steps

- 1) Click  **Generic actions** >  **Export Elements**.
- 2) Select the elements to export.
- 3) Click **Export**.

Export Elements	
Option	Definition
All elements	Exports all elements.
Choose elements	Allows you to select individual elements to export. Type part of the name of an element or browse through the drop-down list to select an element.
Export	Starts the export.

Import elements

Importing elements allows you to reuse or restore elements for single NGFW Engine configuration without having to create them again.

Before you begin

Export elements using the NGFW Manager.



Note

You cannot import elements that were created using the SMC into the NGFW Manager.

Steps

- 1) Click **Generic actions** > **Import Elements**.
- 2) Click **Select element archive**, then browse to the file that contains the exported elements.
- 3) Click **Import elements from archive**.
The import starts.

Back up system configurations

Backups contain the necessary configuration information to restore the NGFW Manager to the state it was in when the backup was taken.

By default, backup files are only stored on the NGFW Engine. We recommend downloading backup files to ensure that the backup files are available if the data on the NGFW Engine is lost.

Steps

- 1) Click **Generic actions** > **Backups**.
- 2) Click **Create backup**.
- 3) (Optional) Enter a name for the backup.
If you do not enter a name, the name is automatically generated.
- 4) Click **Create Backup**.
The backup is created and appears in the list of available backups.

Manage Backups	
Option	Definition
Available backups	Shows backup files that have been created or uploaded to the NGFW Engine.

Option	Definition
...	<p>Actions related to backups.</p> <ul style="list-style-type: none"> 🔄 Restore — Replaces the current NGFW Manager configuration with the configuration from the backup. ⬇️ Download — Saves the backup file on the computer where you are using the NGFW Manager. 🗑️ Delete — Deletes the backup file from the NGFW Engine.
🔄 Create backup	Creates a backup of the current NGFW Manager configuration.
⬆️ Upload backup	Uploads backup files to the NGFW Engine.

Restore backups

Restoring backups allows you to recover from the loss of the system configurations.

Before you begin

Back up system configurations.



CAUTION

Restoring a backup completely replaces the current NGFW Manager configuration with the configuration from the backup. Any elements or configurations that were created after the backup was made are deleted.

Steps

- 1) Click **Generic actions** > **Backups**.
- 2) If the backup that you want to restore is not in the list of available backups, click **Upload backup**, then browse to the backup file.
The backup file is uploaded to the NGFW Engine.
- 3) Next to the backup that you want to restore, click **Generic actions** > **Restore**.
- 4) When prompted to confirm, click **Restore Backup**.
The current NGFW Manager configuration is replaced with the configuration from the backup.

Restart the NGFW Engine

In rare cases, such as when the NGFW Engine is not functioning correctly, you might need to restart the NGFW Engine.



Note

The NGFW Manager user interface is available only after the appliance has finished restarting.

Steps

- 1) Browse to **NGFW > Status**.
- 2) Click **Restart Appliance**.
You are prompted to confirm that you want to restart the appliance.
- 3) Click **Restart Now**.

Result

The appliance restarts. Restarting might take some time.

Turn off the NGFW Engine

You can turn off the NGFW Engine when moving the NGFW appliance to another location, or when doing hardware maintenance.



Note

After you turn off the appliance, you must manually turn on the appliance before you can use it again.

Steps

- 1) Browse to **NGFW > Status**.
- 2) Click **Turn off Appliance**.
You are prompted to confirm that you want to turn off the appliance.
- 3) Click **Turn off Now**.

Result

The appliance turns off.

Collect information for Forcepoint support

When instructed to do so by Forcepoint support, you can collect information about the system to assist in troubleshooting.

Steps

- 1) Browse to **NGFW > Status**.
- 2) Click **Information for Support**.
You are prompted to confirm that you want to collect information for support.
- 3) Click **Get Information Now**.
A file that contains information about the system is created.
- 4) Provide the file to Forcepoint support.

Reset the NGFW appliance to default settings

We recommend resetting the NGFW appliance to default settings before disposing of the appliance, or mailing the appliance to Forcepoint support or another location.

Resetting the NGFW appliance to factory settings ensures that the NGFW appliance does not contain sensitive information.



CAUTION

All data and settings are deleted when you reset the NGFW Engine to default settings.

Steps

- 1) Browse to **NGFW > Status**.
- 2) Click **Reset to Default Settings**.
You are prompted to confirm that you want to reset the NGFW Engine to default settings.
- 3) Click **Reset Now**.

Result

All data and settings are deleted from the NGFW appliance.

