Next Generation Firewall

How to deploy Forcepoint NGFW in the Azure cloud

6.3
Revision B
Introduction

You can deploy Forcepoint NGFW in the Microsoft Azure cloud to provide VPN connectivity, access control, and inspection for networks in the Azure cloud.

After deployment, you can manage NGFW Engines in the Azure cloud using the Management Client component of the Forcepoint NGFW Security Management Center (SMC) in the same way as other NGFW Engines.

Note: Networking in Microsoft Azure is significantly different compared to traditional networking. Deploying Forcepoint NGFW in the Microsoft Azure cloud requires familiarity with networking in Microsoft Azure. For more information about virtual networks in Microsoft Azure, see https://docs.microsoft.com/en-us/azure/virtual-network/.

For more information about using Azure, see the Microsoft Azure Documentation at https://docs.microsoft.com/en-us/azure/.

Licensing models for Forcepoint NGFW in the Azure cloud

Two licensing models are supported for Forcepoint NGFW in the Azure cloud.

- Bring Your Own License — You pay only Microsoft Azure’s standard runtime fee for the NGFW Engine instance. You must install a license for the NGFW Engine in the Forcepoint NGFW Security Management Center (SMC).

- Hourly (pay as you go license) — You pay Microsoft Azure’s standard runtime fee for the NGFW Engine instance plus an hourly license fee based on the runtime of the NGFW Engine. No license installation is needed for the NGFW Engine in the SMC.

For features that require separate licenses, the SMC automatically detects which licensing model the NGFW Engine uses.
Limitations of Forcepoint NGFW in the Azure cloud

There are some limitations on features and configuration options when deploy Forcepoint NGFW in the Microsoft Azure cloud.

- Only single NGFW Engines in the Firewall/VPN role are supported. Clustered NGFW Engines are not supported. Engines in the IPS and Layer 2 Firewall roles are not supported.
- Master NGFW Engines and Virtual Security Engines are not supported.
- The following types of interfaces are not supported: aggregated link interfaces, VLAN interfaces, wireless interfaces, ADSL interfaces.
- FIPS mode is not supported.
- Memory dump diagnostics are not supported.
- Forcepoint NGFW solution templates do not support password authentication for SSH connections to the NGFW Engine command line. You must use SSH keys for authentication of SSH connections to the NGFW Engine command line.

Note: To prevent the same traffic from matching the policy in Azure and the policy in the SMC, do not use an Azure access control list (ACL) or Network security group (NSG), or use an NSG with an Allow All policy for NGFW Engines deployed in the Azure cloud.

Configure the SMC

Configure the network connections and contact addresses for the SMC.

These steps provide an overview of the SMC configuration process. For detailed instructions, see the following documents:

- Forcepoint Next Generation Firewall Installation Guide
- Forcepoint Next Generation Firewall Product Guide

Steps

1) To make sure that your Management Server is reachable from your Forcepoint NGFW instance in Azure, configure the network connections for the SMC in one of these ways:
   - Deploy the SMC on a virtual machine in Azure so that the management connection stays within the private Azure network.
   - Route the management connection over the Internet.

2) Create a Location element for elements that are located in networks outside of the local network of the SMC servers.
3) Configure contact addresses for the Management Server.

   a) In the Management Server Properties dialog box, click Exceptions.
   b) Click Add, select the Location element that you created, then click Select.
   c) In the Contact Addresses cell, enter the external IP address of the Management Server, then click OK.
   d) Click OK to close the Management Server Properties dialog box.

4) Configure contact addresses for the Log Server.
   a) In the Log Server Properties dialog box, click Exceptions.
   b) Click Add, select the Location element that you created, then click Select.
   c) In the Contact Addresses cell, enter the external IP address of the Log Server, then click OK.
   d) Click OK to close the Log Server Properties dialog box.
Configure NGFW Engines

Add and configure a Single Firewall element for each NGFW Engine that you deploy in the Azure cloud. These steps provide an overview of the NGFW Engine configuration process. For detailed instructions, see the following documents:

- Forcepoint Next Generation Firewall Installation Guide
- Forcepoint Next Generation Firewall Product Guide

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

1) Add a Single Firewall element.

2) In the General branch of the Engine Editor, select the Location element for elements outside of the local network of the SMC servers from the Location drop-down list.

3) Select Interfaces, then add a layer 3 physical interface and a dynamic IP address.
   a) Add a layer 3 physical interface.
   b) Add an IPv4 address to the interface.
   c) From the IP address type drop-down list, select Dynamic.
   d) From the Dynamic Index drop-down list, select First DHCP Interface.
   e) Select Automatic Default Route.

4) Select Interfaces > Loopback, then add the following loopback IP address: 127.0.0.1.

5) Select Interfaces > Interface Options, then make the following selections:
   a) Select Interface ID 0 as the primary control interface.
      The Node-Initiated Contact to Management Server option is automatically selected when the control IP address is dynamic. When the option is selected, the NGFW Engine opens a connection to the Management Server and maintains connectivity.
   b) Select the loopback IP address as the identifiy for authentication requests.

6) Select Routing, then add a default route through Interface 0.
   a) Right-click the network under Interface 0, then select Add Router.
   b) Right-click the Router element, then select Add.
   c) Browse to Networks > Any Network, click Add, then click OK.

7) Click Save to save and validate changes, then close the Engine Editor.

8) (Bring your own license only) Install a license, then bind the license to the Single Firewall element.
9) Save the initial configuration.
   a) Right-click the NGFW Engine, then select Configuration > Save initial Configuration.

   b) Next to the Initial Security Policy field, click Select, then select a policy for the NGFW Engine.

   c) Select Enable SSH Daemon.

   d) To save the initial configuration file, click Save As, then select the location where you want to save the file.

Deploy Forcepoint NGFW using a solution template

The Forcepoint NGFW solution template includes the NGFW Engine software and the network environment in which it runs.

The template creates the following routes in Azure through the NGFW Engine:

- A route from external networks to the protected networks
- A route from the protected networks to the Internet

Steps

1) Create a Forcepoint NGFW instance using the custom Forcepoint NGFW solution template.
   a) In the Azure portal, navigate to Virtual Machines > Compute.
b) Click Add, then search for the custom Forcepoint NGFW solution template.

**Tip:** Enter `forcepoint` as a search string to find all solution templates published by Forcepoint.

c) Select a custom Forcepoint NGFW solution template, then click Create.

2) Configure the options in the Basics section.

a) In the NGFW Admin Username field, enter a user name for the administrator account that is used to make SSH connections to the NGFW Engine.

b) In the Admin SSH Public Key field, enter or paste the public key that is used to make SSH connections to the NGFW Engine.

c) From the Subscription drop-down list, select the account that is charged for resources.

d) In the Resource group options, select Create new, then enter a name for the resource group.

e) (Optional) From the Location drop-down list, select the region where you want to deploy the NGFW Engine.

Regions are physical Microsoft Azure data centers. For more information, see [https://azure.microsoft.com/en-us/overview/datacenters/how-to-choose/](https://azure.microsoft.com/en-us/overview/datacenters/how-to-choose/).

f) Click OK.

3) Configure the options in the NGFW Configuration section.

a) (Optional) From the NGFW Version drop-down list, select the NGFW Engine version.

The most recent NGFW Engine version is selected by default.

b) From the Licensing Mode options, select the licensing mode for the NGFW Engine.

c) (Optional) If the default value of the NGFW VM Size option does not meet your needs, select a different value.

d) From the Accelerated Networking options, select On or Off according to your needs.

**Note:** Accelerated networking is only available when you use a virtual machine size that supports it.

e) (Optional) If the default value of the Virtual network option does not meet your needs, select a different value.

f) Next to the Upload initial contact file engine.cfg field, click the file browser icon, then select the engine.cfg file that contains the initial configuration for the NGFW Engine.
4) Configure subnets for the NGFW instance.

   Note: You must view and accept the subnet settings even if you do not change the settings.

   a) If the default settings do not meet your needs, change the settings.
      The default settings are automatically configured based on the initial configuration for the NGFW Engine.

   b) Click OK.

5) Click OK.
   The deployment continues to a summary and the configuration is validated.

6) When the validation is finished, click OK.

7) Review the terms of use, then click Purchase.

Result
The NGFW Engine deployment starts. When deployment is finished, you can check the status and manage the NGFW Engine using the Management Client.

Configure a VPN with an NGFW Engine in Azure

When you have deployed an NGFW Engine in Azure, you can use it as an endpoint in VPNs with other NGFW Engines in your network.

Configuring a VPN between NGFW Engines that are managed by the same SMC has the following advantages compared to using Azure’s native VPN tools:

- Access control for VPN traffic
- Centralized management of the NGFW Engines that act as VPN gateways

Because the public IP addresses of NGFW Engines deployed in Azure are dynamic, the following restrictions apply when you use an NGFW Engine deployed in Azure as a VPN gateway:

- The VPN gateway must be use some other identifier than the IP address, such as DNS name, email address, or (if certificate authentication is used) the certificate’s Distinguished Name (DN) as the phase-1 ID.
- IKEv1 main mode with pre-shared key authentication is not supported. Aggressive mode allows the use of pre-shared keys, but for security reasons certificate-based authentication is also recommended when IKEv1 is set in aggressive mode.
**Configure the NGFW Engine deployed in Azure as a VPN gateway**

Configure settings for the NGFW Engine deployed in Azure that allow you to use it as a VPN gateway.

**Steps**

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

1) In the Azure portal, select your virtual machine, then select Overview to find the DNS name of your NGFW Engine.

2) In the Management Client, add the DNS name of the NGFW Engine to the dynamic IP address under interface 0.
   a) Right-click the NGFW Engine, then select Edit <element type>.
   b) In the navigation pane on the left, select Interfaces.
   c) Right-click the IP address, then select Edit IP Address.
   d) In the Contact Addresses options, enter the DNS name of your NGFW Engine in the Default field.
   e) Click OK.

3) Configure the phase-1 ID of the VPN endpoint.
   a) In the navigation pane on the left, select VPN > End-Points.
   b) Right-click the internal endpoint, then select Properties.
   c) In the Phase-1 ID settings, select one of the following options from the ID Type drop-down list, then enter a value in the ID Value field according to the type.
      - DNS Name — Enter the DNS name of your NGFW Engine.
      - Email — Enter an email address identifies the gateway.
      - Distinguished name — Enter the Distinguished Name (DN) that is used in the gateway's certificate.
   d) Click OK.

4) Click Save.

**Define a policy-based VPN**

To a policy-based VPN, first you define some basic properties for the VPN, then you add gateways. These steps provide an overview of the VPN configuration process. For detailed instructions, see the Forcepoint Next Generation Firewall Product Guide.
How to deploy Forcepoint NGFW in the Azure cloud

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

1) Select Configuration, then browse to VPN.

2) Browse to Policy-Based VPNs.

3) Right-click Policy-Based VPNs, then select New Policy-Based VPN.

4) In the Name field, enter a name for the VPN.

5) (Optional) From the Default VPN Profile drop-down list, select the VPN Profile element that defines the settings for authentication, integrity checking, and encryption.

6) Click OK.
   The Policy-Based VPN opens for editing.

7) On the Site-to-Site VPN tab, drag and drop the gateways that you want to include in this VPN into either of the two panes for the VPN topology.
   • To allow a gateway to establish a VPN tunnel with any other gateway in the VPN, add it to the Central Gateways pane.
   • To allow a gateway to establish a VPN tunnel only with central gateways in this VPN, add it to the Satellite Gateways pane.

8) Click Save.

9) Add Access rules and possibly also NAT rules to direct outgoing traffic to the VPN and allow incoming traffic from the VPN.

Find product documentation

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

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