



FlexEdge Secure SD- WAN

7.1

**How to deploy Secure SD-WAN
in the Azure cloud**

Contents

- Introduction
- Configure the SMC
- Deploy a single Secure SD-WAN Engine using automatic deployment
- Deploying Cloud Auto-Scaled Firewalls
- Deploy Forcepoint FlexEdge Secure SD-WAN using manual deployment
- Configure a VPN with an FlexEdge Secure SD-WAN Engine in Azure
- Forcepoint FlexEdge Secure SD-WAN High Availability with Azure Resource Manager
- Find product documentation

Introduction

You can deploy Forcepoint FlexEdge Secure SD-WAN in the Microsoft Azure cloud to provide VPN connectivity, access control, and inspection for networks in the Azure cloud.

After deployment, you can manage Secure SD-WAN Engines in the Azure cloud using the Management Client component of the Forcepoint FlexEdge Secure SD-WAN Manager in the same way as other Secure SD-WAN Engines.



Important

Networking in Microsoft Azure is significantly different compared to traditional networking. Deploying Forcepoint FlexEdge Secure SD-WAN 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/>.

Product name change

This release introduces change to product and component names. For more information about the change to product and component names, refer to the **About this Help** section in the *Forcepoint FlexEdge Secure SD-WAN Product Guide*.



Important

- 1) Some documentations, knowledge base articles, and other support information are still using the old product name.
- 2) There is no change in the Engine local user interface.
- 3) The IPS role has transitioned now from L2FW mode to L3FW mode.

Deprecated features

The following features are no longer supported:

- SSL VPN Portal.
- Web Portal User Interface is deprecated and is not available by default.

For more information on deprecated features, refer to the **About this release** section in the *FlexEdge Secure SD-WAN Manager 7.1.0 Release Notes*.

Licensing models for Forcepoint FlexEdge Secure SD-WAN in the Azure cloud

Two licensing models are supported for Forcepoint FlexEdge Secure SD-WAN in the Azure cloud.

- **Bring Your Own License** — You pay only Microsoft Azure's standard runtime fee for the Secure SD-WAN Engine instance. You must manually install the license for the Secure SD-WAN Engine in the Forcepoint FlexEdge Secure SD-WAN Manager is automatically installed.
- **Hourly (pay as you go license)** — You pay Microsoft Azure's standard runtime fee for the Secure SD-WAN Engine instance plus an hourly license fee based on the runtime of the Secure SD-WAN Engine. No license installation is needed for the Secure SD-WAN Engine in the SMC.

For features that require separate licenses, the SMC automatically detects which licensing model the Secure SD-WAN Engine uses.

Provisioning methods for Forcepoint FlexEdge Secure SD-WAN in the Azure cloud

Two provisioning methods are supported for Forcepoint FlexEdge Secure SD-WAN in the Azure cloud.

- **Automatic** — The FlexEdge Secure SD-WAN solution template automatically creates the Secure SD-WAN Engine in the Forcepoint FlexEdge Secure SD-WAN Manager using the SMC API when you deploy Forcepoint FlexEdge Secure SD-WAN in the Azure cloud. You can use automatic deployment to create single Secure SD-WAN Engines and Cloud Auto-Scaled Firewalls.
To use automatic deployment, you must configure the SMC API in the Management Client before you deploy Forcepoint FlexEdge Secure SD-WAN in the Azure cloud.
- **Manual** — You must configure the Secure SD-WAN Engine elements in the SMC before you deploy Forcepoint FlexEdge Secure SD-WAN in the Azure cloud. When you use manual deployment, you must upload the configuration file generated for the Secure SD-WAN Engine in the SMC to the Azure cloud.

Limitations of Forcepoint FlexEdge Secure SD-WAN in the Azure cloud

There are some limitations on features and configuration options when you deploy Forcepoint FlexEdge Secure SD-WAN in the Microsoft Azure cloud.



CAUTION

To protect the privacy of your data, we recommend using an instance type that runs on dedicated hardware, such as an isolated instance.

- Only single Secure SD-WAN Engines in the Engine/VPN role are supported. Clustered Secure SD-WAN Engines are not supported. Engines in the IPS and Layer 2 Engine roles are not supported.
- Master Secure SD-WAN 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 FlexEdge Secure SD-WAN solution templates do not support password authentication for SSH connections to the Secure SD-WAN Engine command line. You must use SSH keys for authentication of SSH connections to the Secure SD-WAN Engine command line.

Interfaces and routing for Forcepoint FlexEdge Secure SD-WAN in the Azure cloud

Interfaces and routing in the Azure cloud work differently than in physical networks. To understand how interfaces and networking work in the Azure cloud, we recommend that you familiarize yourself with the concept of Azure User Defined Routes.

For more information, see the following Microsoft Azure documentation:

- <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>
- <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface-vm#constraints>



When you deploy Forcepoint FlexEdge Secure SD-WAN in the Azure cloud, the solution template automatically creates a security subnet, a front end subnet, and a back end subnet. The interface and routing configuration is similar to the configuration that is shown in this example: <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-dmz-nsg-fw-udr-asm>

The Secure SD-WAN Engine has one interface in the security subnet. The route table created by the solution template sends all traffic for the Secure SD-WAN Engine to the interface in the security subnet. The Secure SD-WAN Engine does not need to have interfaces in the front end subnet or the back end subnet to communicate with them.

Configure the SMC

Before you deploy Forcepoint FlexEdge Secure SD-WAN in the Microsoft Azure cloud, prepare the SMC for the deployment.

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

- [Forcepoint FlexEdge Secure SD-WAN Installation Guide](#) 
- [Forcepoint FlexEdge Secure SD-WAN Product Guide](#) 

Configure network connections and contact addresses for the SMC


Make sure that your Management Server and Log Server are reachable from your Forcepoint FlexEdge Secure SD-WAN instance in Azure.


You must always configure network connections and contact addresses for the SMC, regardless of whether you use automatic deployment or manual deployment.



Note

For FlexEdge Secure SD-WAN 6.4, the default contact addresses must be the external IP addresses of the Management Server and the Log Server. Make sure that the external IP addresses of the Management Server and the Log Server are reachable from the Internet.

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

- 1) Create a Location element for elements that contact the SMC servers using a different IP address than the default contact address.
 - a) Select  **Configuration**, then browse to **Administration**.
 - b) Browse to **Other Elements > Locations**.
 - c) Right-click **Locations**, then select **New Location**.
 - d) Add the elements to the **Content** pane.
 - For FlexEdge Secure SD-WAN 6.4, add elements that contact the SMC servers using the internal IP addresses of the SMC servers.
 - For FlexEdge Secure SD-WAN 6.5 and higher, add Secure SD-WAN Engine elements that contact the SMC servers using the external IP addresses of the SMC servers.
 - e) Click **OK**.
 - f) In the properties of the Secure SD-WAN Engine elements or other elements that you added, select this Location.

- 2) Select **Dashboard > Servers / Devices**, then browse to **Management Server**.
- 3) Right-click the Management Server, then select **Properties**.

The screenshot shows the 'Management Server - Properties' dialog box. The 'General' tab is selected. The 'Name' field contains 'Management Server'. The 'IPv4 Address' field contains '10.0.254.199'. The 'IPv6 Address' field contains '<Enter IPv6>'. The 'Location' dropdown is set to 'Not Specified'. The 'Contact Addresses' section has a 'Default' field with '10.0.254.199' and a 'remote' field with 'vpn: 10.66.1.2'. The 'Log Server' dropdown is set to 'Log Server'. The 'RADIUS Method' dropdown is set to 'EAP-MD5'. The 'TACACS Method' dropdown is set to 'MSCHAP'. The 'Include in Database Replication' checkbox is checked. The 'Category' dropdown is set to 'Not Categorized'. The 'Tools Profile' dropdown is set to '<Select>'. The 'Comment' field is empty. Buttons for 'Resolve', 'Exceptions...', 'Select...', and 'OK' are visible.

- 4) In the **Default** field in the **Contact Addresses** section, enter the default contact address for the Management Server.
 - For FlexEdge Secure SD-WAN 6.4, enter the external IP address of the Management Server.
 - For FlexEdge Secure SD-WAN 6.5 and higher, enter the internal IP address of the Management Server.
- 5) To configure contact address exceptions for the Management Server, click **Exceptions**.
- 6) Click **Add**, select the Location element that you created, then click **Select**.
- 7) In the **Contact Addresses** cell, enter the IP address, then click **OK**.
 - For FlexEdge Secure SD-WAN 6.4, enter the internal IP address of the Management Server.
 - For FlexEdge Secure SD-WAN 6.5 and higher, enter the external IP address of the Management Server.
- 8) Click **OK** to close the **Management Server Properties** dialog box.
- 9) Browse to **Log Server**, right-click the Log Server, then select **Properties**.

- 10) In the **Default** field in the **Contact Addresses** section, enter the default contact address for the Log Server.
 - For FlexEdge Secure SD-WAN 6.4, enter the external IP address of the Log Server.
 - For FlexEdge Secure SD-WAN 6.5 and higher, enter the internal IP address of the Log Server.
- 11) To configure contact address exceptions for the Log Server, click **Exceptions**.
- 12) Click **Add**, select the Location element that you created, then click **Select**.
- 13) In the **Contact Addresses** cell, enter the IP address, then click **OK**.
 - For FlexEdge Secure SD-WAN 6.4, enter the internal IP address of the Log Server.
 - For FlexEdge Secure SD-WAN 6.5 and higher, enter the external IP address of the Log Server.
- 14) Click **OK** to close the **Log Server Properties** dialog box.

Create a self-signed certificate for the SMC API

If you plan to deploy Forcepoint FlexEdge Secure SD-WAN using automatic deployment, create a self-signed certificate for the SMC API.



Note

The certificate for the SMC API must be self-signed. Do not use externally signed certificates for the SMC API.

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


- 1) Select ⚙ **Configuration**, then browse to **Administration**.
- 2) Browse to **Certificates > TLS Credentials**.
- 3) Right-click **TLS Credentials**, then select **New TLS Credentials**.
- 4) In the **Name** field, enter a unique name for the certificate.
- 5) In the **Common Name** field, enter the fully qualified domain name (FQDN) or IP address that the SMC API service uses.
- 6) Add the same FQDN or IP address that you entered in the Common Name field as the Subject Alternative Name.
 - a) Click **Edit** next to the **Subject Alternative Name** field.
 - b) Click **Add**, then select the correct type from the drop-down list in the **Type** cell. If the value is an IP address, then select IP as the type. If the value is an FQDN, then select DNS as the type.


- c) Double-click the **Value** cell, then enter the same FQDN or IP address that you entered in the **Common Name** field.
- 7) From the signing options, select **Self-Sign**, then click **Finish**.
- 8) Right-click the certificate element, then select **Properties**.
- 9) On the **Certificate** tab, click **Export**, then save the certificate file.

Enable the SMC API

If you plan to deploy Forcepoint FlexEdge Secure SD-WAN using automatic deployment, enable the SMC API and create an SMC API Client account.

These tasks provide an overview of the SMC API configuration process. For more information, see the *Forcepoint FlexEdge Secure SD-WAN Manager API User Guide* [↗](#).


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

- 1) Select  **Dashboard** > **Servers / Devices**, then browse to **Management Server**.
- 2) Right-click the Management Server, then select **Properties**.
- 3) On the **SMC API** tab, select **Enable**.
- 4) In the **Host Name** field, enter the same FQDN or IP address that is used in the certificate for the SMC API.
- 5) (Optional) To use a port other than the default port, enter the port number in the **Port Number** field. The default port number is 8082.



Note

If you enter a different port number here, you must also specify the port number when you configure the **Forcepoint FlexEdge Secure SD-WAN provisioning** settings in the Azure portal.

- 6) (Optional) If the Management Server has several addresses and you want to restrict access to one address, specify the IP address to use in the **Listen Only on Address** field.
- 7) To enable the use of HTTPS for SMC API connections, click **Select** next to the **Server Credentials**, then select the TLS Credentials element that contains the certificate for the SMC API.
- 8) Create an SMC API Client.
 - a) Select  **Configuration**, then browse to **Administration**.
 - b) Browse to **Access Rights**.

- c) Right-click **Access Rights**, then select **New > API Client**.
- d) In the **Name** field, enter a name for the API Client element.
- e) Use the automatically generated authentication key or click **Generate Authentication Key** to generate a new one.



Important

This key appears only once, so make sure to record the value in the **Authentication Key** field. You must enter this key when you configure the **Forcepoint FlexEdge Secure SD-WAN provisioning** settings in the Azure portal.

- f) On the **Permissions** tab, select **Unrestricted Permissions (Superuser)**.

Deploy a single Secure SD-WAN Engine using automatic deployment

When you use automatic deployment, Secure SD-WAN Engine elements are automatically created in the SMC.

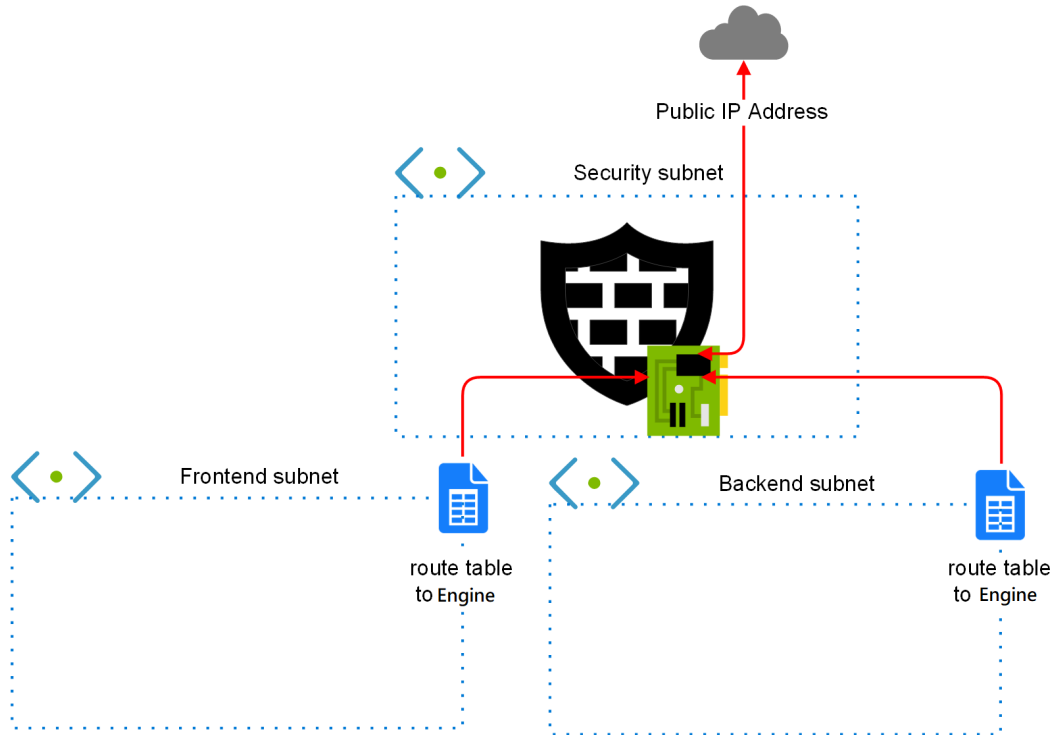
Before you begin

Configure the SMC and enable the SMC API. The SMC API must be reachable from the Internet.

To use automatic deployment, Forcepoint FlexEdge Secure SD-WAN 6.4 or higher is required.

The Forcepoint single FlexEdge Secure SD-WAN solution template includes the Secure SD-WAN Engine software and the network environment in which it runs. The network environment includes the Security subnet in which the Secure SD-WAN Engine is deployed, and two protected subnets. The template creates a route from the protected subnets to the Internet through the Secure SD-WAN Engine. A route is also created between the two protected subnets.

Network environment for single Secure SD-WAN engine deployment



Start the automatic deployment

To start the automatic deployment, create a Forcepoint FlexEdge Secure SD-WAN instance using an Forcepoint FlexEdge Secure SD-WAN solution template.

Steps

- 1) In the Azure dashboard, click **Create a resource**.
- 2) In the Azure Marketplace pane, search for the NGFW solution template.



Tip

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

- 3) Select the Forcepoint single NGFW solution template, then click **Create**.

Configure basic settings for the Forcepoint FlexEdge Secure SD-WAN instance

Configure settings for how to connect to the Forcepoint FlexEdge Secure SD-WAN instance, and where to deploy the instance.

Steps

- 1) In the **NGFW Admin Username** field, enter a user name for the administrator account that is used to make SSH connections to the Secure SD-WAN Engine.
- 2) In the **Admin SSH Public Key** field, enter or paste the public key that is used to make SSH connections to the Secure SD-WAN Engine.
- 3) From the **Subscription** drop-down list, select the account that is charged for resources.
- 4) In the **Resource group** options, select **Create new**, then enter a name for the resource group.



Note

You must always create a new resource group for the deployment. It is not possible to use an existing resource group.

- 5) (Optional) From the **Location** drop-down list, select the region where you want to deploy the Secure SD-WAN Engine.
Regions are physical Microsoft Azure data centers. For more information, see <https://azure.microsoft.com/en-us/overview/datacenters/how-to-choose/>.



Note

When you use an hourly (pay as you go) license, only Microsoft tax remitted countries and regions are supported. For more information, see Knowledge Base article [16011](#).

- 6) Click **OK**.

Configure FlexEdge Secure SD-WAN settings

Configure settings for the virtual machine where the Forcepoint FlexEdge Secure SD-WAN instance runs.

Steps

- 1) From the **NGFW licensing model** options, select the licensing model for the Secure SD-WAN Engine.
- 2) (Optional) From the **NGFW Version** drop-down list, select the Secure SD-WAN Engine version.
Version 6.4 or higher is required.
- 3) If the default value of the **Virtual network** option does not meet your needs, select a different value.
You must view and accept the virtual network settings even if you do not change the settings.
- 4) If the default values of the **NGFW Security Subnet**, **Protected FrontEnd Subnet**, and **Protected BackEnd Subnet** options do not meet your needs, change the settings, then click **OK**.

- 5) (Optional) If the default value of the **NGFW VM Size** option does not meet your needs, select a different value.
We recommend selecting a general purpose VM size that has a SKU that starts with the letter D and at least 4 GB of RAM.
- 6) In the **Resource prefix** field, enter an identifying prefix that is automatically added to the name of the resource.
The prefix is also added to the name of the automatically created Secure SD-WAN Engine element in the SMC.
- 7) From the **VM Zone** options, select the zone to which the Secure SD-WAN Engine belongs.
- 8) From the **Modify existing vnet to redirect traffic to NGFW** option, select whether to automatically redirect traffic to the Secure SD-WAN Engine.



Note

The **Modify existing vnet to redirect traffic to NGFW** options are only available if you selected an existing virtual network as the value of the **Virtual network** option. If you created a new virtual network for the FlexEdge Secure SD-WAN deployment, the new virtual network is automatically configured.

- **Yes** — Traffic to and from the protect subnets is immediately redirected to the Secure SD-WAN Engine. Route tables are automatically attached to the virtual networks that are selected for the **Protected FrontEnd Subnet** and **Protected BackEnd Subnet** options. For Cloud Auto-Scaled Firewalls, the mandatory Azure NSG is deployed in the virtual network that you selected for the **NGFW Security Subnet** option.



Note

If additional subnets need to be redirected to the Secure SD-WAN Engine, you must associate the route table manually with those additional subnets.

- **No** — You must associate route tables with the virtual networks that are selected for the **Protected FrontEnd Subnet** and **Protected BackEnd Subnet** options to route traffic through the Secure SD-WAN Engine. For Cloud Auto-Scaled Firewalls, you must manually attach the mandatory Azure NSG to the virtual network that you selected for the **NGFW Security Subnet** option.

- 9) Click OK.

Configure FlexEdge Secure SD-WAN provisioning and finish the automatic deployment

The FlexEdge Secure SD-WAN provisioning settings enable the connection between the Forcepoint FlexEdge Secure SD-WAN instance and the SMC API, and define settings that are applied after the instance starts.

Steps

- 1) From the **NGFW Deployment model** drop-down list, select **Automatic via SMC REST API**.
- 2) In the **SMC Contact address (FQDN or IP address)** field, enter the fully qualified domain name (FQDN) or the public IP address of the SMC API.

Make sure that the information that you enter here matches the common name or subject alternative name in the certificate for the SMC API.



Tip

You can find the FQDN or IP address of the SMC API in the **Host Name** field on the **SMC API** tab of the **Management Server Properties** dialog box in the Management Client.

- 3) (Optional) If the SMC API uses a port other than the default port, enter the SMC API port number in the **SMC rest API port** field.

The default port number is 8082.

- 4) In the **SMC rest API key** field, enter the authentication key of the SMC API Client.

- 5) Make sure that **Yes** is for **Check REST API TLS certificate options**.

When **Yes** is selected, the TLS certificate of the SMC API is validated when Secure SD-WAN Engine elements are automatically created.



Note

The **No** option is intended only for testing purposes. We do not recommend selecting **No** in a production environment.

- 6) Next to the **Upload SMC rest API certificate** field, click the file browser icon, then select the certificate file.



Tip

To find the certificate in the Management Client, select **Configuration**, then browse to **Administration > Certificates > TLS Credentials**.

- 7) (FlexEdge Secure SD-WAN 6.5 and higher) In the **Engine Location** field, enter the name of the Location element that is selected for the Secure SD-WAN Engine when the Secure SD-WAN Engine element is created.

The Location element must already exist before you deploy the Secure SD-WAN Engine. The name must match the name of the Location element in the SMC.



Note

Make sure that you have defined contact address exceptions for this location in the properties of the Management Server and the Log Server.

- 8) (Recommended) In the **Engine policy name** field, enter the name of the Engine Policy that is uploaded to the Secure SD-WAN Engine after the Secure SD-WAN Engine element is created.

The Engine Policy must already exist before you deploy the Secure SD-WAN Engine. The name must match the name of the Engine Policy element in the SMC.



Note

If you do not specify a Engine Policy, you must manually install a policy using the Management Client after deploying the Secure SD-WAN Engine.

- 9) (Optional) From the **Engine Auto delete when shutting off** options, select **No** if you want the Secure SD-WAN Engine element to stay in the SMC when the Secure SD-WAN Engine instance shuts down. When **Yes** is selected, the Secure SD-WAN Engine elements are automatically deleted when the Secure SD-WAN Engine instances shut down or are restarted in Azure.
- 10) Click **OK**.
The deployment continues to a summary and the configuration is validated.
- 11) When the validation is finished, click **OK**.
- 12) Review the terms of use, then click **Create**.

Result

The Secure SD-WAN Engine deployment starts and an Secure SD-WAN Engine element is automatically created in the SMC. When deployment is finished, you can check the status using the Management Client.

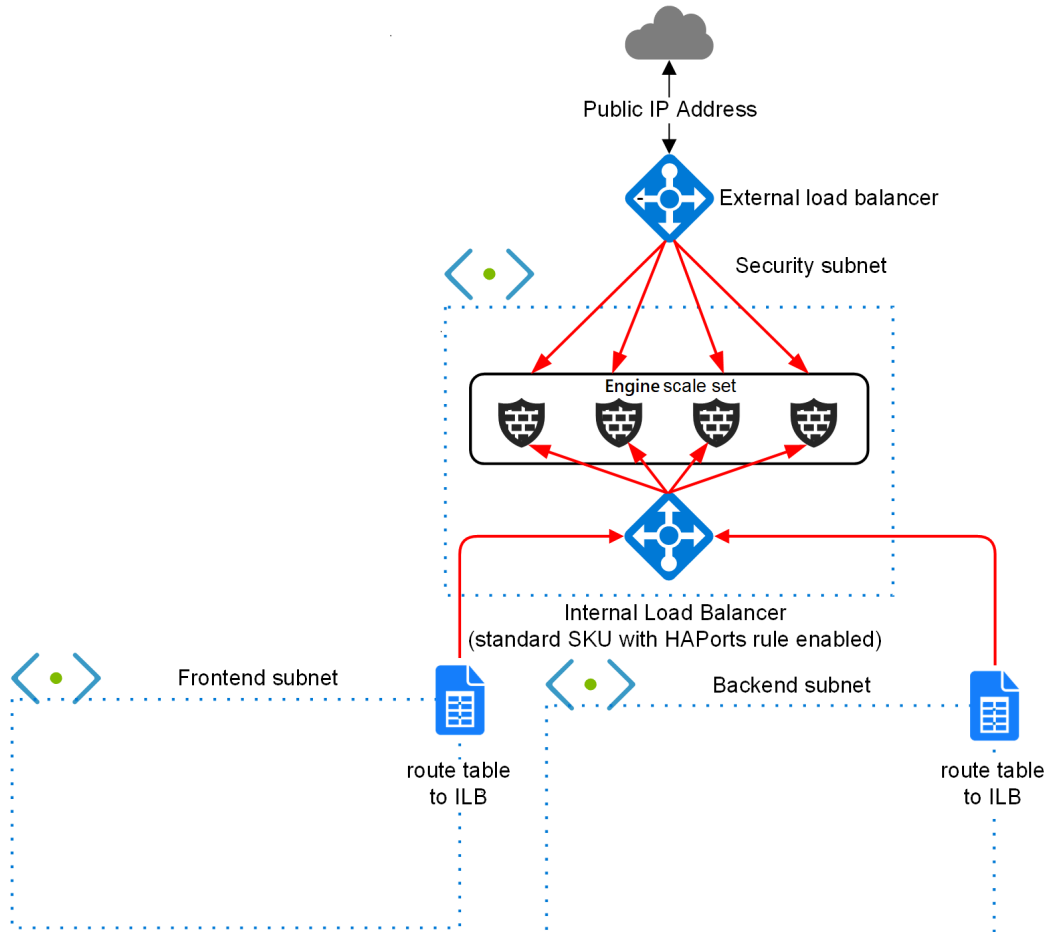
Deploying Cloud Auto-Scaled Firewalls

You can create Secure SD-WAN Engines that can be scaled manually, on a schedule, or automatically depending on traffic load.

Using scaling features is an advanced task. You must know how scaling works and be aware of the related Azure guidelines. For Forcepoint FlexEdge Secure SD-WAN, both vertical and horizontal scaling is supported. For more information about scaling in Azure, see <https://docs.microsoft.com/en-us/azure/architecture/best-practices/auto-scaling>.

The scale set Secure SD-WAN solution template includes the Secure SD-WAN Engine software and the network environment in which it runs. The network environment includes the Security subnet in which the Secure SD-WAN Engines are deployed, and two protected subnets. The template creates a route from the protected subnets to the Internet through the Secure SD-WAN Engines. A route is also created between the two protected subnets.

Network environment for Cloud Auto-Scaled Firewall deployment



Cloud Auto-Scaled firewalls have the following limitations:

- Cloud Auto-Scaled Firewalls can only be created for Forcepoint FlexEdge Secure SD-WAN 6.4 or higher.
- The hourly (pay as you go) licensing model is recommended for Cloud Auto-Scaled Firewalls.
- The SMC API is required for Cloud Auto-Scaled Firewalls.
- Because you cannot modify the properties of Cloud Auto-Scaled Firewalls in the SMC, features that require changing the properties of the Secure SD-WAN Engine elements are not supported.

Monitoring Cloud Auto-Scaled Firewalls in the Management Client

Cloud Auto-Scaled Firewalls are automatically added to Cloud Auto-Scaled Firewall Groups, and the groups are shown in the Home view.

You can preview the Cloud Auto-Scaled Firewalls in the Engine Editor, but you cannot make changes to the configuration.

You can make changes to the installed policy and refresh the policy on the Cloud Auto-Scaled Firewalls, but you cannot install a different policy.

Start the deployment of Cloud Auto-Scaled Firewalls

To deploy a Cloud Auto-Scaled Firewall, use automatic deployment to create a Secure SD-WAN instance using the scale set Secure SD-WAN template.

Before you begin

To deploy Cloud Auto-Scaled Firewalls, Forcepoint FlexEdge Secure SD-WAN 6.4 or higher is required.

Steps

- 1) In the Azure dashboard, click **Create a resource**.
- 2) In the Azure Marketplace pane, search for the NGFW solution template.



Tip

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

- 3) Select the scale set NGFW solution template, then click **Create**.

Configure basic settings for the Cloud Auto-Scaled Firewalls

Configure settings for how to connect to the Cloud Auto-Scaled Firewalls, and where to deploy the instances.

Steps

- 1) In the **NGFW Admin Username** field, enter a user name for the administrator account that is used to make SSH connections to the Secure SD-WAN Engine.
- 2) In the **Admin SSH Public Key** field, enter or paste the public key that is used to make SSH connections to the Secure SD-WAN Engine.
- 3) From the **Subscription** drop-down list, select the account that is charged for resources.
- 4) In the **Resource group** options, select **Create new**, then enter a name for the resource group.



Note

You must always create a new resource group for the deployment. It is not possible to use an existing resource group.

- 5) (Optional) From the **Location** drop-down list, select the region where you want to deploy the Secure SD-WAN Engine.

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



Note

When you use an hourly (pay as you go) license, only Microsoft tax remitted countries and regions are supported. For more information, see Knowledge Base article [16011](#).

- 6) Click **OK**.

Configure FlexEdgeSecure SD-WAN settings for the Cloud Auto-Scaled Firewalls

Configure settings for the virtual machines where the Cloud Auto-Scaled Firewalls run.

Steps

- 1) (Optional) From the **NGFW Version** drop-down list, select the Secure SD-WAN Engine version. Version 6.4 or higher is required.

- 2) From the **NGFW licensing model** options, select **Pay as you go**.



Note

The hourly (pay as you go) licensing model is recommended for Cloud Auto-Scaled Firewalls. If you use the bring your own license licensing model, you must have an Secure SD-WAN license in the SMC for each Secure SD-WAN Engine that is automatically created.

- 3) If the default value of the **Virtual network** option does not meet your needs, select a different value. You must view and accept the virtual network settings even if you do not change the settings.
- 4) If the default values of the **NGFW Security Subnet**, **Protected FrontEnd Subnet**, and **Protected BackEnd Subnet** options do not meet your needs, change the settings, then click **OK**.
- 5) In the **Resource prefix** field, enter an identifying prefix that is automatically added to the name of the resource.
The prefix is also added to the name of the automatically created Secure SD-WAN Engine elements in the SMC.
- 6) In the **Initial instance count in the Autoscale group** field, enter the number of Secure SD-WAN Engine elements that are automatically created when the Cloud Auto-Scaled Firewalls start.
- 7) Click **OK**.

Configure FlexEdge Secure SD-WAN provisioning and finish deploying Cloud Auto-Scaled Firewalls

The FlexEdge Secure SD-WAN provisioning settings enable the connection between the Cloud Auto-Scaled Engine instances and the SMC API, and define settings that are applied after each instance starts.

Steps

- 1) In the **SMC Contact address (FQDN or IP address)** field, enter the fully qualified domain name (FQDN) or the public IP address of the SMC API.
Make sure that the information that you enter here matches the common name or subject alternative name in the certificate for the SMC API.



Tip

You can find the FQDN or IP address of the SMC API in the **Host Name** field on the **SMC API** tab of the **Management Server Properties** dialog box in the Management Client.

- 2) (Optional) If the SMC API uses a port other than the default port, enter the SMC API port number in the **SMC rest API port** field.
The default port number is 8082.
- 3) In the **SMC rest API key** field, enter the authentication key of the SMC API Client.
- 4) Make sure that **Yes** is for **Check REST API TLS certificate options**.
When **Yes** is selected, the TLS certificate of the SMC API is validated when Secure SD-WAN Engine elements are automatically created.



Note

The **No** option is intended only for testing purposes. We do not recommend selecting **No** in a production environment.

- 5) Next to the **Upload SMC rest API certificate** field, click the file browser icon, then select the certificate file.



Tip

To find the certificate in the Management Client, select **Configuration**, then browse to **Administration > Certificates > TLS Credentials**.

- 6) (FlexEdge Secure SD-WAN 6.5 and higher) In the **Engine Location** field, enter the name of the Location element that is selected for the Secure SD-WAN Engine when the Secure SD-WAN Engine element is created.

The Location element must already exist before you deploy the Secure SD-WAN Engine. The name must match the name of the Location element in the SMC.



Note

Make sure that you have defined contact address exceptions for this location in the properties of the Management Server and the Log Server.

- 7) (Recommended) In the **Engine policy name** field, enter the name of the Engine Policy that is uploaded to the Secure SD-WAN Engine after the Secure SD-WAN Engine element is created.

The Engine Policy must already exist before you deploy the Secure SD-WAN Engine. The name must match the name of the Engine Policy element in the SMC.



Note

If you do not specify a Engine Policy, you must manually install a policy using the Management Client after deploying the Secure SD-WAN Engine.

- 8) (Optional) From the **Engine Auto delete when shutting off** options, select **No** if you want the Secure SD-WAN Engine elements to stay in the SMC when the Secure SD-WAN Engine instances shut down or are restarted in Azure.

When **Yes** is selected, the Secure SD-WAN Engine elements are automatically deleted when the Secure SD-WAN Engine instances shut down or are restarted in Azure.

If you select **No**, you must manually remove unused Cloud Auto-Scaled Engines in the Management Client.

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

We recommend selecting a general purpose VM size that has a SKU that starts with the letter D and at least 4 GB of RAM.

- 10) Click **OK**.

The deployment continues to a summary and the configuration is validated.

- 11) When the validation is finished, click **OK**.

- 12) Review the terms of use, then click **Create**.

- 13) Add one or more load balancing rules and configure scaling for the Cloud Auto-Scaled Firewalls.

For instructions, see the Microsoft Azure documentation at <https://docs.microsoft.com/en-us/azure/>.



Result

The Secure SD-WAN Engine deployment starts and Secure SD-WAN Engine elements are automatically created in the SMC. When deployment is finished, you can check the status using the Management Client. You can preview the Secure SD-WAN Engine properties in the Engine Editor, but you cannot make changes to the configuration.

Add NAT rules for Cloud Auto-Scaled Firewalls

To prevent asymmetric routing, add NAT rules in the Management Client.

Steps

- 1) Select  **Configuration**.
- 2) Browse to **Policies > Engine Policies**, then open your Engine Policy for editing.
- 3) On the **IPv4 NAT** tab, add the a rule, then define the source, destination, and service:
 - **Source** — ANY
 - **Destination** — \$\$ DHCP Interface 1.ip Alias element
 - **Service** — Select the service according to the type of traffic that the Secure SD-WAN Engine handles.
- 4) To define source and destination translation, double-click the **NAT** cell.
- 5) On the **Source Translation** tab, configure source NAT.
 - a) From the **Translation Type** drop-down menu, select **Dynamic**.
 - b) Next to the **IP Address Pool** field, click **Select**.
 - c) Browse to the \$\$ DHCP Interface 1.ip Alias element, then click **Select**.
 - d) Deselect **Automatic Proxy ARP**.
- 6) On the **Destination Translation** tab, configure destination NAT.
 - a) Select **Translate Destination**.
 - b) Next to the **Translated** field, click **IP Address**, then enter the destination IP address in the protected network.
For example, if the destination is a web server in the protected network, enter the private IP address of the web server.
 - c) Deselect **Automatic Proxy ARP**.
- 7) Click **OK**.
- 8) Click  **Save and Install**.

Remove unused Cloud Auto-Scaled Firewalls

If you do not set the template solution parameter to automatically remove Cloud Auto-Scaled Firewall instances, you must periodically remove them in the Management Client.

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

- 1) Select ⚙ **Configuration**.
- 2) Browse to **Other Elements > Cloud Auto-Scaled Groups**.
- 3) Right-click a Cloud Auto-Scaled Group, then select **Tools > Remove Unused Cloud Auto-Scaled Firewalls**.
- 4) Click **OK**.

Deploy Forcepoint FlexEdge Secure SD-WAN using manual deployment

When you use manual deployment, you must create Secure SD-WAN Engine elements in the SMC before you deploy the Secure SD-WAN Engine in the Azure cloud environment.

Create the Secure SD-WAN Engine in the Management Client

If you are deploying using the single Secure SD-WAN Engine, add and configure a placeholder Single Engine element for each Secure SD-WAN Engine that you deploy in the Azure cloud.


These steps provide an overview of the Secure SD-WAN Engine configuration process. For detailed instructions, see the following documents:

- [Forcepoint FlexEdge Secure SD-WAN Installation Guide](#) ⓘ
- [Forcepoint FlexEdge Secure SD-WAN Product Guide](#) ⓘ

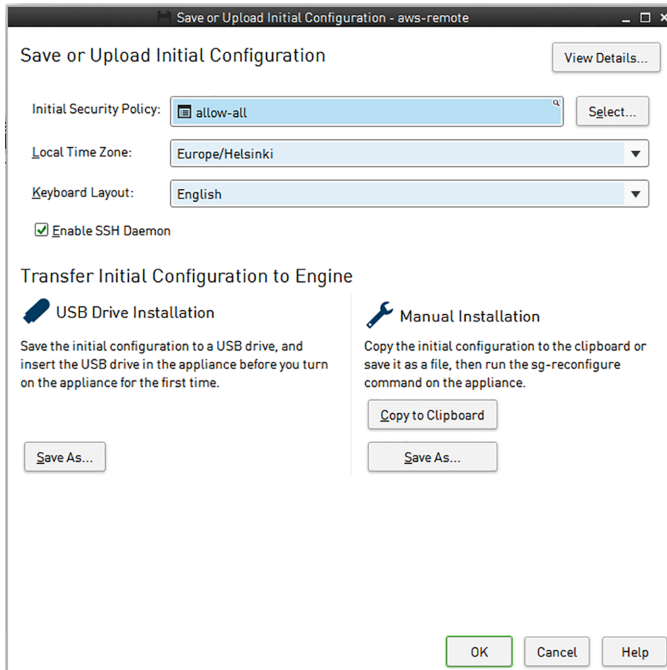
Steps ⓘ For more details about the product and how to configure features, click **Help** or press **F1**.

- 1) Add a Single Engine element.
- 2) Browse to the **General** branch of the Engine Editor, then select the Location element for elements outside of the local network of the SMC servers from the **Location** drop-down list.

- 3) Browse to **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) Browse to **Interfaces > Loopback**, then add the following loopback IP address: 127.0.0.1.
- 5) Browse to **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 Secure SD-WAN Engine opens a connection to the Management Server and maintains connectivity.
 - b) Select the loopback IP address as the identify for authentication requests.
- 6) Browse to **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 Engine element.

- 9) Save the initial configuration.
 - a) Right-click the Secure SD-WAN Engine, then select **Configuration > Save initial Configuration**.



- b) Next to the **Initial Security Policy** field, click **Select**, then select a policy for the Secure SD-WAN 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 the Secure SD-WAN Engine in the Azure cloud environment

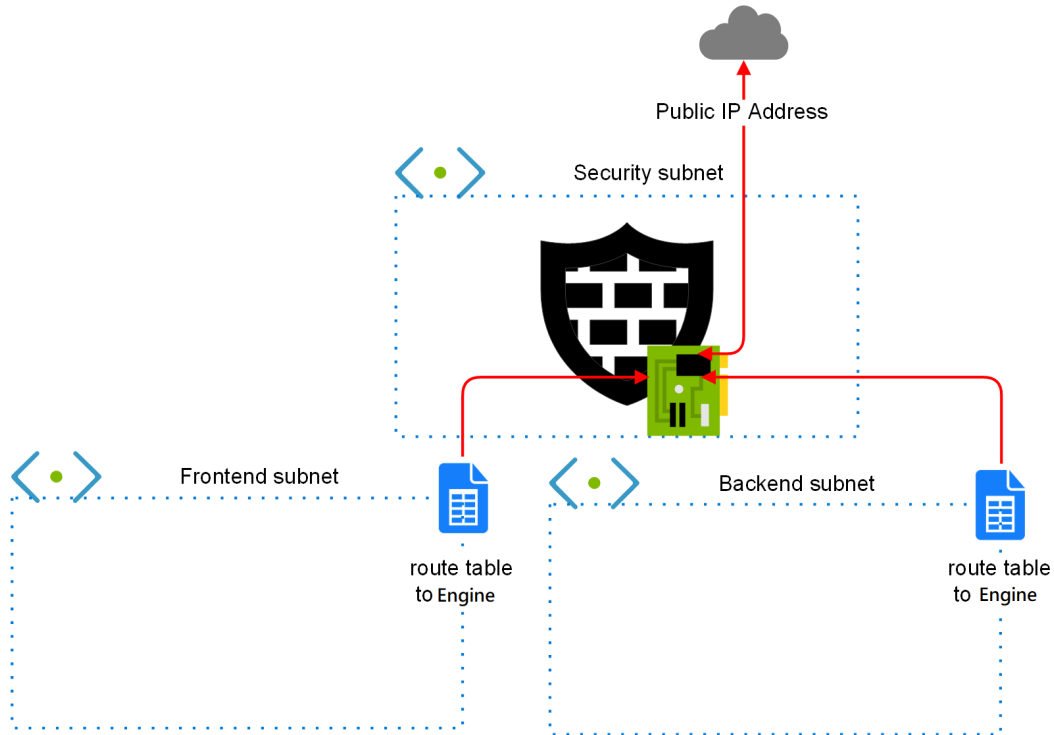
The Forcepoint single FlexEdge Secure SD-WAN solution template includes the Secure SD-WAN Engine software and the network environment in which it runs.

Before you begin

Configure the SMC and add an Secure SD-WAN Engine element in the Management Client.

The network environment includes the Security subnet in which the Secure SD-WAN Engine is deployed, and two protected subnets. The template creates a route from the protected subnets to the Internet through the Secure SD-WAN Engine. A route is also created between the two protected subnets.

Network environment for single Secure SD-WAN engine deployment



Steps

- 1) Create a Secure SD-WAN instance using the Forcepoint single Secure SD-WAN solution template.
 - a) In the Azure dashboard, click **Create a resource**.
 - b) In the Azure Marketplace pane, search for the NGFW solution template.



Tip

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

- c) Select the Forcepoint single 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 Secure SD-WAN Engine.
 - b) In the **Admin SSH Public Key** field, enter or paste the public key that is used to make SSH connections to the Secure SD-WAN 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.



Note

You must always create a new resource group for the deployment. It is not possible to use an existing resource group.

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

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



Note

When you use an hourly (pay as you go) license, only Microsoft tax remitted countries and regions are supported. For more information, see Knowledge Base article [16011](#).

- f) Click **OK**.

3) Configure the options in the **Secure SD-WAN configuration** section.

- a) From the **NGFW licensing model** options, select the licensing model for the Secure SD-WAN Engine.

- b) (Optional) From the **NGFW Version** drop-down list, select the Secure SD-WAN Engine version. Version 6.4 or higher is required.

- c) If the default value of the **Virtual network** option does not meet your needs, select a different value.

- d) If the default values of the **NGFW Security Subnet**, **Protected FrontEnd Subnet**, and **Protected BackEnd Subnet** options do not meet your needs, change the settings, then click **OK**.

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

We recommend selecting a general purpose VM size that has a SKU that starts with the letter D and at least 4 GB of RAM.

- f) From the **VM Zone** options, select the zone to which the Secure SD-WAN Engine belongs.

- g) From the **Modify existing vnet to redirect traffic to NGFW** option, select whether to automatically redirect traffic to the Secure SD-WAN Engine.



Note

The **Modify existing vnet to redirect traffic to NGFW** options are only available if you selected an existing virtual network as the value of the **Virtual network** option. If you created a new virtual network for the FlexEdge Secure SD-WAN deployment, the new virtual network is automatically configured.

- **Yes** — Traffic to and from the protect subnets is immediately redirected to the Secure SD-WAN Engine. Route tables are automatically attached to the virtual networks that are selected for the **Protected FrontEnd Subnet** and **Protected BackEnd Subnet** options. For Cloud Auto-Scaled Firewalls, the mandatory Azure NSG is deployed in the virtual network that you selected for the **NGFW Security Subnet** option.
 - **No** — You must associate route tables with the virtual networks that are selected for the **Protected FrontEnd Subnet** and **Protected BackEnd Subnet** options to route traffic through the Secure SD-WAN Engine. For Cloud Auto-Scaled Firewalls, you must manually attach the mandatory Azure NSG to the virtual network that you selected for the **NGFW Security Subnet** option.
- h) Click **OK**.
- 4) Configure the options in the **Secure SD-WAN provisioning** section.
- a) From the **Secure SD-WAN Deployment model** drop-down list, select **Manual via engine.cfg**.
 - b) 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 Secure SD-WAN Engine.
- 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 **Create**.

Result

The Secure SD-WAN Engine deployment starts. When deployment is finished, you can check the status and manage the Secure SD-WAN Engine using the Management Client.

Configure a VPN with an FlexEdge Secure SD-WAN Engine in Azure

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



Note

You cannot use Cloud Auto-Scaled Engines in VPNs.

Configuring a VPN between Secure SD-WAN 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 Secure SD-WAN Engines that act as VPN gateways

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


- The VPN gateway must use the fully qualified domain name (FQDN) of your Secure SD-WAN Engine 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 Secure SD-WAN Engine deployed in Azure as a VPN gateway

Configure settings for the Secure SD-WAN 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 FQDN of your Secure SD-WAN Engine.
- 2) (Secure SD-WAN 6.4 only) In the Management Client, add the FQDN of the Secure SD-WAN Engine to the dynamic IP address under interface 0.
For Secure SD-WAN 6.5 or higher, the FQDN is entered automatically.
 - a) Right-click the Secure SD-WAN 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 FQDN of your Secure SD-WAN 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 **SD-WAN > End-Points**.
 - b) Right-click the internal endpoint, then select **Properties**.
 - c) In the **Phase-1 ID** settings, select **DNS Name** from the **ID Type** drop-down list, then enter the FQDN of your Secure SD-WAN Engine in the **ID Value** field.
 - 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 FlexEdge Secure SD-WAN Product Guide* [↗](#).

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

- 1) Select  **Configuration**, then browse to **Secure SD-WAN**.
- 2) Browse to **Policy-Based SD-WAN**.
- 3) Right-click **Policy-Based SD-WAN**, then select **New Policy-Based SD-WAN**.
- 4) In the **Name** field, enter a name for the SD-WAN.
- 5) (Optional) From the **Default SD-WAN Profile** drop-down list, select the SD-WAN Profile element that defines the settings for authentication, integrity checking, and encryption.
- 6) Click **OK**.

The Policy-Based SD-WAN opens for editing.
- 7) On the **Site-to-Site SD-WAN** 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.

Forcepoint FlexEdge Secure SD-WAN High Availability with Azure Resource Manager

This section provides detailed instructions to deploy and configure Forcepoint Secure SD-WAN Engine using a high availability topology (Active-Active mode) in Azure. This deployment is done using an Azure Resource Manager (ARM) template.

Forcepoint-VM for Azure supports active/passive high availability (HA) configuration. When the Forcepoint-VM detects a failure, the passive engine instance becomes active and uses Azure API calls to configure its interfaces/ports.

This Azure Resource Manager (ARM) template lets system administrators to automatically:

- Deploy two standalone Forcepoint Secure SD-WAN engines.
- Configure engines to operate in Active-Active mode and to report to an existing Forcepoint Secure SD-WAN Manager (SMC).
- Deploy and configure all Azure network components involved in the stack.

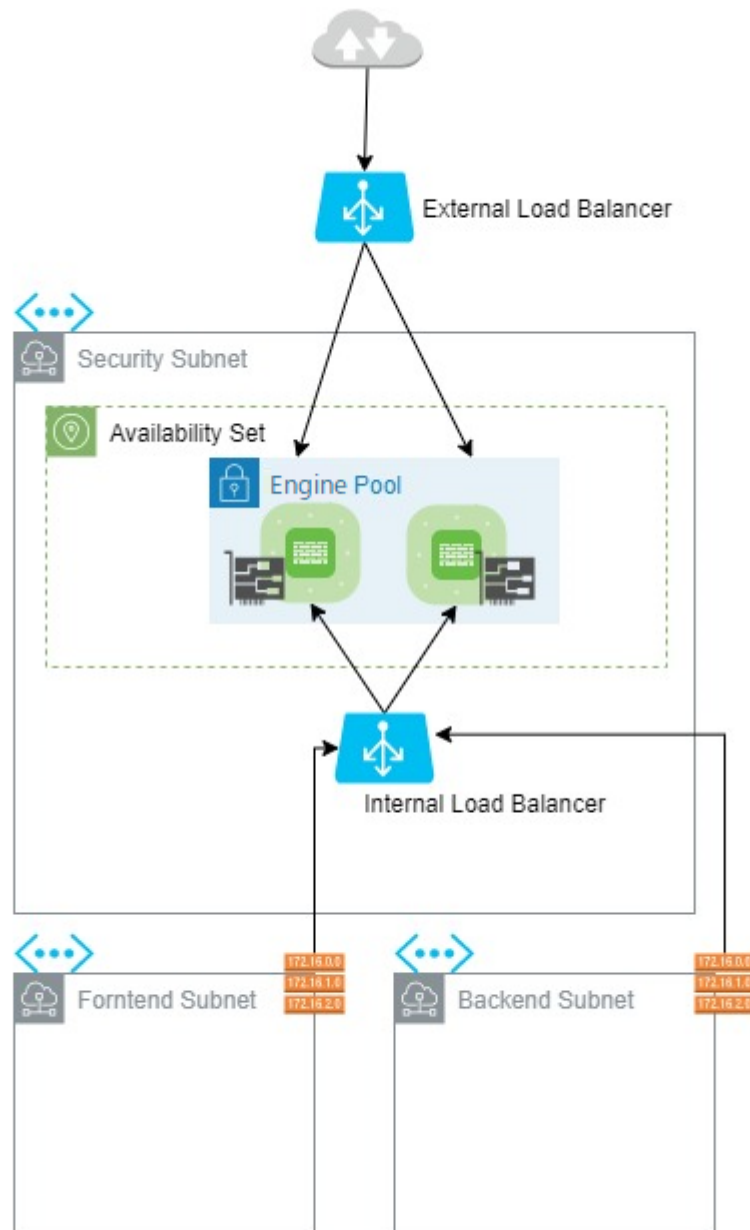
The ARM template is designed to deploy and configure the following resources within the Azure account of the user:

- External Load Balancer (Internet-facing).
- Internal Load Balancer.
- Virtual Networks (if not already existing) with 3 subnets: **subnet-0-security**, **subnet-1-front** and **subnet-2-back**.

Subnets **subnet-1-front** and **subnet-2-back** are used to connect user workloads.

- Two instances of Forcepoint Secure SD-WAN engines either in the same **Availability Zone** using **Availability Sets**, or into two different **Availability Zones**.
- Two NICs one for each Forcepoint Secure SD-WAN engine.
- Azure components instrumental to operate the entire stack: Storage accounts, Route Tables, Security Groups and Public IP addresses

The following diagram provides a description of the workflow between the components involved in this solution:



Prerequisites

Make sure to meet the following prerequisites in order to deploy and configure Secure SD-WAN using a high availability topology (Active-Active mode) in Azure

- Azure account with active subscription.
- Forcepoint Secure SD-WAN Manager with a public FQDN or IP address.
- A Windows machine with PowerShell (used to convert TLS certificates).

The system administrator can also include the following maintenance procedures in this deployment workflow:

- To appropriately handle logs produced during any step of the solution workflow.
- To monitor scripts, services, and applications involved in the solution.

Configure Secure SD-WAN Manager

The following procedures let you to configure Secure SD-WAN Manager:

Create a self-signed certificate for the Secure SD-WAN Manager API

- 1) Login to your SMC machine.
- 2) Select **Configuration** and navigate to **Administration**.
- 3) Select **Certificates > TLS Credentials**.
- 4) Right-click **TLS Credentials**, and then select **New TLS Credentials**.
- 5) In the **Name** field, enter a unique name for the certificate.
- 6) In the **Common Name** field, enter the fully qualified domain name (FQDN) or the public IP address that the SMC API service uses.
- 7) Add the same FQDN or IP address that you entered in the **Common Name** field as the **Subject Alternative Name**.
- 8) Click **Edit** option next to the **Subject Alternative Name** field.
 - If you have a fully qualified domain name (FQDN), do the following:
 - Click **Add**
 - Select **DNS** from the drop-down list in the **Type** cell,
 - Double-click **Value** cell, then enter the FQDN.
 - If you use a public IP address to access the SMC API, do the following:
 - Click **Add**,
 - Select **IP address** from the drop-down list in the **Type** cell,
 - Double-click **Value** cell, then enter the public IP address for SMC API connections.
- 9) From the signing options, select **Self-Sign**, and then click **Finish**.
- 10) Right-click the certificate element as created in the preceding steps.
- 11) Select **Properties**.
- 12) On the **Certificate** tab, click **Export** and save the certificate file.
- 13) Click **OK**.
- 14) Convert the exported certificate to **base64 string** using a Windows machine with **Windows PowerShell ISE**.

- 1) Open **Windows PowerShell ISE** and load the content of the exported certificate into a variable. Using the following command, replace the red text with the path to the exported certificate:
- 2) `$pfx_cert = get-content 'C:\Users\Demo\Downloads\certificate1604078668615.crt' -Encoding Byte`
- 3) Run the following command to convert the exported certificate to **Base64 string**:
- 4) `[System.Convert]::ToBase64String($pfx_cert)`
- 5) Save the output in a secure location for future reference.

Enable the SMC API

- 1) Login to the SMC portal.
- 2) Select **Dashboard > Servers / Devices**, then browse to **Management Server**.
- 3) Right-click the **Management Server**, then select **Properties**.
- 4) On the **SMC API** tab, select **Enable**.
- 5) In the **Host Name** field, enter the FQDN or public IP address for SMC that is used in the certificate for the SMC API.
- 6) Click **Select** next to the **Server Credentials**, and then select the **TLS Credentials** element that contains the certificate you have created for the SMC API.
- 7) Click **OK**, and then click **Yes**.

Create an SMC API Client

- 1) Select **Configuration** and navigate to **Administration**.
- 2) Navigate to **Access Rights**.
- 3) Right-click **API Clients** then select **New API Client**.
- 4) In the **Name** field, enter a name for the **API Client** element.
- 5) You can either use the automatically generated authentication key or click **Generate Authentication Key** to generate a new one. This key appears only once, so make sure to save the value in the **Authentication Key** field in a secure location since it will be needed in the next steps described in this document.
- 6) On the **Permissions** tab, select **Unrestricted Permissions (Superuser)**.
- 7) Select **Configuration** and navigate to **Administration**.

- 8) Click **OK**.

Create a Location element

To create location element for elements that contact the SMC servers.

- 1) Select **Configuration** and navigate to **Administration**.
- 2) Browse to **Other Elements > Locations**.
- 3) Right-click **Locations** and select **New Location**.
- 4) Enter a name in the **Name** field.
- 5) Click **OK**.

Configure Management Server

- 1) Select **Dashboard > Servers / Devices**, then browse to **Management Server**.
- 2) Right-click the **Management Server**.
- 3) Select **Properties**.
- 4) In the **Default** field of **Contact Addresses** section, enter the default contact address for the **Management Server**
 - For Secure SD-WAN 6.4, enter the external (public) IP address of the Management Server.
 - For Secure SD-WAN 6.5 and higher, enter the internal IP address of the Management Server.
- 5) Click **Exceptions > Add**
- 6) Select the Location element that you created, and then click **Select**.
- 7) In the **Contact Addresses** cell, enter the IP address then click **OK**.
 - For Secure SD-WAN 6.4, enter the internal IP address of the Management Server
 - For Secure SD-WAN 6.5 and higher, enter the external (public) IP address of the Management Server.
- 8) Click **OK** to close the Management Server **Properties** dialog box, and then click **Yes**.

Configure Log Server

- 1) Navigate to **Others > Log Server**.
- 2) Right-click **Log Server**, and then select **Properties**.

- 3) In the **Default** field in the **Contact Addresses** section, enter the default contact address for the Log Server.
 - For Secure SD-WAN 6.4, enter the external IP address of the Log Server.
 - For Secure SD-WAN 6.5 and higher, enter the internal IP address of the Log Server.
- 4) To configure contact address exceptions for the Log Server, click **Exceptions**.
- 5) Click **Add**, select the **Location** element that you created, then click **Select**.
- 6) In the **Contact Addresses** cell, enter the IP address, then click **OK**.
 - For Secure SD-WAN 6.4, enter the internal IP address of the Log Server.
 - For Secure SD-WAN 6.5 and higher, enter the external IP address of the Log Server.
- 7) Click **OK** to close the Log Server **Properties** dialog box and then click **Yes**.

Create Engine Policy

This section is optional, if your existing Secure SD-WAN Manager already includes a **Engine Policy** that you want to apply to the engines deployed in Azure.

To create a Engine Policy:

- 1) Select **Configuration > Secure SD-WAN > Policies**.
- 2) Right-click **Policies** and select **New > Engine Policy**.
- 3) Give a name to your **Engine policy**.
- 4) Select **Engine Template**.
- 5) Click **OK**.

Configure Azure and deploy the template

The following procedures let you to configure Secure SD-WAN Manager:

Create Azure Resource Group for Forcepoint Secure SD-WAN High Availability

- 1) Sign into the Azure portal using the link <https://portal.azure.com/>.
- 2) Click **Resource groups**.
- 3) Click **Add**.
- 4) Enter the following values:

- **Subscription:** select your Azure subscription.
 - **Resource group:** enter a new resource group name.
 - **Region:** select an Azure location.
- 5) Click **Review + Create**.
 - 6) Click **Create**. It takes few moments to create a **Resource Group**.

Download Secure SD-WAN high availability ARM template

- 1) Download the **fp-ngfw-ha-arm-template.tar.gz** from <https://frcpnt.com/fp-ngfw-ha-arm-template-latest>.
- 2) Untar the **fp-ngfw-ha-arm-template.tar.gz** with the following command:

```
tar -zxvf fp-ngfw-ha-arm-template.tar.gz
```

The output consists of a directory named **fp-ngfw-ha-arm-template**, which contains the following two .json files:

- **fp-ngfw-ha-template.json**
- **fp-gfw-ha.parameters.json**

Edit and deploy the template to Azure Resource Management

- 1) From the search box in the Azure portal menu, type **deploy**, and then select **Deploy a custom template**.
- 2) Under **Custom deployment > Select a template**, select **Build your own template in the editor** option in to create a customized template.
- 3) Select **Load file**, and browse the file system to upload the **fp-ngfw-ha-template.json** file, included in the **fp-ngfw-ha-arm-template** directory. For more information, see *Download Forcepoint Secure SD-WAN high availability ARM template*.
- 4) Click **Save**.
- 5) Under **Custom deployment > Basics**, select **Edit parameters**.
- 6) Select **Load file**, and browse the file system to upload the **fp-ngfw-ha-parameters.json** file, included in the **fp-ngfw-ha-arm-template** directory. For more information, see *Download Forcepoint Secure SD-WAN high availability ARM template*.
Make sure not to click **Save** after uploading the parameter file.
- 7) Once you have loaded the parameter file into parameters editor, edit the following parameters:
 - **Line 6: Parameters.location.value:** the name of the Azure Region where the resources will be deployed.

- **Line 9: Parameters.engineUsername.value:** username that will be used to login into Forcepoint Secure SD-WAN engine VMs.
- **Line 12: parameters.sshkey.value:** Secure SD-WAN engine username public ssh key. To find more about how to generate ssh keys, visit: <https://docs.microsoft.com/en-us/azure/virtual-machines/linux/mac-create-ssh-keys>.
- **parameters.vnet:** these parameters represent the **Virtual Network (VNet)** for the deployment. If the VNet does not exist it will be created. User needs to specify the name for the VNet and its **Resource Group**.
- If the VNet exists, change the value **vnet.value.newOrExisting** to **existing**. Modify the other VNet **addressPrefix** and **subnets names** parameters to not overlap with existing subnets **addressPrefix**.
- **line 45: parameters.sku.value:** choose the type of Secure SD-WAN licensing model. Options are
 - **Pay as you go:** enter the value `ngfw_payg`
 - **Bring your own license:** enter the value `ngfw_byol`. If this option is used, the Secure SD-WAN engines will pull a license from the ones available in the SMC.
- **Line 48: parameters.ImageVersion.value:** the version for the Forcepoint Secure SD-WAN engine image.
- **Line 51: parameters.engineVMSize.value:** the size of the Azure VM. The size must be available in the Azure region selected for the deployment.
- **Line 57: parameters.smcContactAddress.value:** enter the public IP address or FQDN of the SMC API.
- **Line 63: parameters.smcContactApikey.value:** enter the SMC API key generated in the section **Enable the SMC API**.
- **Line 69: Parameters.smcCertificate.value:** enter the Bas64 string for the certificate created in the section **Create a self-signed certificate for the SMC API** of this document.
- **Line 72: parameters.ploicyName.value:** enter the **Policy** name created in the section *Create Engine Policy* of this document.
- **Line 78: parameters.engineLocation.value:** enter the engine **Location** name created in the section **Create a Location element for elements that contact the SMC servers**.
- **Line 81: parameters.logServerPool.value:** the name of the **Log Servers** as displayed inside Secure SD-WAN Manager.
- **Line 86: parameters.useZones.value:** set the value to **true** to use **Availability Zones** of Azure.



Note

Not all Azure locations provide availability zones. Set the value to **false** if the stack is deployed in a location that does not support availability zones. In such situation, **Availability Set** will be used to deploy both Secure SD-WAN engines in the same data center within different fault domains and update domains.

- If **parameters.useZones.value** is set to **true**, you need to choose two different availability zones, one for each Forcepoint Secure SD-WAN engine instance.
- 8) Once all parameters are defined, click **Save** to save all changes made to the parameters file.
 - 9) Select the Resource group you have created.
 - 10) Click **Review + create**.
 - 11) Click **Create** to start the deployment.

The deployment might take few moments to finish. Once complete, the following message is displayed:

```
"Your deployment is complete".
```

Once deployment is completed, two Secure SD-WAN Engines will be displayed inside Forcepoint SMC.

Troubleshooting

Follow these steps to identify issues impacting the normal operation of the integration:

Validate the prerequisites

Make sure the following prerequisites as described in the Introduction are met:

- Secure SD-WAN Manager with a public FQDN or IP address.
- A Windows machine with PowerShell (used to convert TLS certificate).
- Using the following command, the user can download the file:

```
wget -content-disposition https://frcpnt.com/fp-ngfw-ha-arm-template-latest
```

Check network connectivity

Make sure Engines or other security appliances are not impacting the network connectivity necessary for the operation of all components involved in this integration:

- Run the following command on the host machine to check internet connectivity:

```
ping -c 2 <SMC public IP here>
```

The result must be similar to the following sample:

```
PING <SMC public IP> (10.10.120.12) 56(84) bytes of data.
```

```
64 bytes from 10.10.120.12 (10.10.120.12): icmp\ _seq=1 ttl=128 time=179 ms
```

```
64 bytes from 10.10.120.12 (10.10.120.12): icmp\ _seq=1 ttl=128 time=181 ms
```

Check all components are configured and running properly

Make sure the products and services are configured as expected and are running. Verify the Azure deployment is completed with no errors. The deployment takes few moments to complete:

Once deployment is completed, two Secure SD-WAN Engines will be displayed inside Forcepoint SMC. Validate the network configuration of the newly deployed stack as described in the **End to end test** section.

Secure SD-WAN Engine versions available in Azure

To find Secure SD-WAN Engine versions available in Azure, perform the following steps:

- 1) Sign into the Azure portal using the link <https://portal.azure.com/>.
- 2) In the search bar on top of the portal enter **Marketplace** and click it once displayed in the results.
- 3) In the search bar of the Marketplace, type **Forcepoint Next** and click **Forcepoint Next Generation Firewall**.
- 4) Click the tile named **Forcepoint Next Generation Firewall** and select **Forcepoint single NGFW**.
- 5) Click **Create**.
- 6) Select **NGFW Configuration** option in the creation wizard.
- 7) Select **NGFW Engine version** from the drop-down menu. This displays all available NGFW versions that can be deployed with the Azure Resource Manager template.

Example

To ensure configuration is done properly and both the Forcepoint Secure SD-WAN Engines are working fine, follow the following steps to create a test bed.

- 1) Create a Windows Server 16 machine in the **subnet-1-front** subnet.
 - In the Azure portal search for **Virtual Machines** and select **Virtual machines**.
 - Click **Add** and select **Virtual machine**.
 - Select a **Resource Group** for this Virtual Machine.
 - In **Virtual machine name** option, give a name to this virtual machine.
 - For **Region**, select the Azure region where you have deployed the ARM template.
 - For **Image**, select a **Windows Server 2016** image.
 - In the **Administrator account** section, enter a username and a password. Save both in a secure location for future reference.
 - In the **Inbound port rules** section, select **None** for **Public inbound ports**.
 - Click **Next: Disk**.
 - Click **Next: Networking**.
 - Select the Virtual network used (or create if not already existing) by the ARM template.
 - Select the subnet **subnet-1-front**.
 - For the public IP, select **None**.
 - Click **Review + Create**.
 - Click **Create**.

It might take few moments to create the VM.

- 1) Add a rule to the **External Load Balancer** to forward the RDP traffic to its **Backend pool**.
 - In the Azure portal, search for **Load Balancers** and select it.
 - Click the **External Load Balancer** which has been created by the ARM template (the load balancer which ends with **-externallb**)
 - Under the **Setting** section, click **Load balancing rules**

- Click **Add**
 - Give a name to this rule.
 - **For Port**, add **3389**.
 - **For Backend Port**, add **3389**.
 - Click **OK** to save the rule.
- 2) Add a rule to the **Engine Policy** used with the Forcepoint NFW engines to allow RDP to the Windows Server 2016 you have created.
- Login to the Forcepoint SMC.
 - Select **Configurations > Policies > Engine policies** and find the policy used in the ARM template.
 - Right-click on your policy name and select **Edit Engine Policy**.
 - Click **Yes**.
 - Add a new Rule.
 - Define the Engine rule with specific source IPs, so that only the intended user testing the deployment will have access via Remote Desktop to the Windows Server 2016 machine hosted in Azure.
 - Click **IPv4 NAT**.
 - Set **Source** to **ANY**.
 - Set **Destination** to **\$\$ DHCP Interface 1.ip**.
 - Set **Service** to **any**.
 - Right-click **NAT** and select **Edit NAT**.
 - Configure **Source Translation** .
 - Click **Destination Translation**, select **Translate Type** as **Translate Destination**.
 - Click **Translate Destination**.
 - Click on **Address**, enter the private IP address of the Windows Server 2016 VM you have created, and click **OK**.
 - The configuration for **Translate Destination** looks similar to the following sample screenshot:
 - The final configuration for **IPv4 NAT** will look as in the following screenshot:
 - Click the **Save and install** icon, this will deploy the policy to both Forcepoint NFW Engine instances on Azure.
- 3) Login to the Windows Server 2016 using Remote Desktop.
- On any Windows machine, search for Remote Desktop Connection.
 - Enter the DNS name or the public IP address of the **External Load Balancer** and click **Connect**.

If all configuration settings are correct, you need to enter the credentials to login to the Windows Server 2016 machine.

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. To create a customer account, navigate to the Customer Hub Home page, and then click the **Create Account** link.

