Forcepoint Next Generation Firewall

How to deploy Forcepoint Next Generation Firewall in the Amazon Web Services cloud

6.3 and higher
Revision F
Introduction

You can deploy Forcepoint NGFW in the Amazon Web Services (AWS) cloud to provide VPN connectivity, access control, and inspection for services in the AWS cloud.

Forcepoint™ Next Generation Firewall (Forcepoint NGFW) is available in the Amazon marketplace as an Amazon machine image (AMI) that allows you to run a Forcepoint NGFW Engine instance in the Amazon EC2 cloud. You deploy Forcepoint NGFW Engines in the same way as other virtual machines in the Amazon EC2 cloud.

Note: Regions are physical AWS data centers. Regions are isolated instances with their own set of objects and REST API end points. AWS objects are only unique within a region.

Two licensing models are supported for Forcepoint NGFW in the AWS cloud. There are two AMIs, depending on the licensing model:

- Bring Your Own License — You pay only Amazon's standard runtime fee for the engine instance. You must install a license for the engine in the Forcepoint NGFW Security Management Center (SMC).
- Hourly (pay as you go license) — You pay Amazon's standard runtime fee for the engine instance plus an hourly license fee based on the runtime of the engine. No license installation is needed for the engine in the SMC.

For information about supported Forcepoint NGFW versions, see Knowledge Base article 10156.

After deployment, you can manage NGFW Engines in the AWS cloud using the Management Client component of the SMC in the same way as other NGFW Engines. However, there are some limitations on features and configuration options:

- Only single NGFW Engines in the Firewall/VPN role are supported. Clustered 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.
- VLAN interfaces are not supported.
- Link aggregation is not supported.
- FIPS mode is not supported.
- Memory dump diagnostics are not supported.
- The engine does not limit the number of network interfaces but some types of instances might have limitations.
Deploy Forcepoint NGFW using 1-Click Launch

Create a Forcepoint NGFW instance, then deploy the SMC.

Create a Forcepoint NGFW instance using 1-Click Launch

Configure and launch an instance of the Forcepoint NGFW AMI using 1-Click Launch.

⚠️ **CAUTION:** To protect the privacy of your data, we recommend using dedicated instances when you deploy Forcepoint NGFW in AWS.

Steps

1) In the AWS Marketplace, start the launch for the Forcepoint NGFW AMI.

2) On the 1-Click Launch tab, configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Select the most recent version.</td>
</tr>
<tr>
<td>Region</td>
<td>Select the region that is the best match for your existing infrastructure and geographic location.</td>
</tr>
<tr>
<td>EC2 Instance Type</td>
<td>Select an instance type that meets your performance needs. The AMI automatically restricts the instance types so that only compatible instance types are available.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you want to change the instance type later, you must create a new instance.</td>
</tr>
<tr>
<td>VPC Settings</td>
<td>Select a VPC and a subnet that correspond to the management interface of the NGFW Engine.</td>
</tr>
<tr>
<td>Security Group</td>
<td>Select a security group based on the seller settings. If the default security group is too limited for your environment, you can use a different security group or change the rules. You can also configure the NGFW Engine to restrict access.</td>
</tr>
<tr>
<td>Key Pair</td>
<td>Select a key pair for SSH connections to the NGFW engine.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The key is the only allowed authentication method for SSH connections to the engine command line.</td>
</tr>
</tbody>
</table>

3) Click Launch with 1-click.
4) When the instance is running, connect to the command line of the NGFW Engine and verify the SSH server identity.
   a) In the AWS web management console, select the NGFW Engine instance, then select Actions > Instance Settings > Get system log to show the SSH server fingerprints. The SSH server fingerprint are shown at the end of the NGFW Engine boot messages.
   b) On your computer, open a terminal program, then enter the following command to connect to the command line of the NGFW Engine using the aws user account:

   ```
   ssh -i <your ssh private key>.pem aws@<aws instance public ip address>
   ```

   The SSH key fingerprints are shown when you connect.
   c) Compare the SSH key fingerprints to the SSH server fingerprints from the system log.
   d) To confirm that you want to continue connecting, type `yes`. The IP address of the NGFW Engine is added to the SSH known hosts list.

5) To set a sudo password for the aws user, enter the following command:

   ```
   sudo passwd
   ```

   **Note:** AWS does not allow the root user to log in to the command line. Instead, you must log in as the aws user and use sudo to gain root permissions. You must set a password for the aws user before you can use sudo.

---

**Deploy the SMC**

When the NGFW Engine launch is complete, deploy the SMC.

**Before you begin**

To deploy the SMC, you must have a computer with a 64-bit Linux operating system.

**Note:** If you already have existing SMC installation, it is not necessary to install an additional SMC for controlling NGFW Engines deployed in AWS.

**Steps**

1) On the computer where you want to deploy the SMC, open a terminal program, then enter the following command to copy the SMC installation files:

   ```
   scp -p -i <your ssh private key>.pem aws@<aws instance public ip address>:/spool/<smc installation files>.zip .
   ```

2) Decompress the SMC installation files.

3) Navigate to the `<smc installation files>/Forcepoint_SMC_Installer/Linux-x64` directory.
4) To start the SMC installation, enter the following command:

```
sudo ./setup.sh
```

5) Install the SMC components.

For detailed instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.

### 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 documentation:

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

**Steps**

1) Make sure that your Management Server is reachable from your Forcepoint NGFW AWS instance.

2) In the Management Client, create a Location element for elements that are located in networks outside of the local network for the SMC servers.

   In the example configuration, a Location element called "internet" has been created.

3) Configure contact addresses for the Management Server.
In the example configuration, the external IP address that is used to reach the SMC from AWS has been configured as the contact address for the "internet" Location.

**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 Address cell, enter the external IP address that is used to reach the SMC from AWS, 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, then select the Location element that you created and click Select.
c) In the Contact Address cell, enter the external IP address of the Log Server, then click OK.

d) Click OK to close the Log Server Properties dialog box.

Create Single Firewall elements

Create a Single Firewall element for each Forcepoint NGFW engine that you deploy in the AWS cloud.

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

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

Steps

1) Add a Single Firewall element.

2) From the Location drop-down list on the General pane, select the Location element for elements outside of the local network of the SMC servers.
   In the example configuration, the "internet" Location element is used.

3) Add a layer 3 physical interface and configure it as the primary control interface.
   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 DCHP Interface.
   e) In the Interface Options, 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 engine opens a connection to the Management Server and maintains connectivity.

4) Add more physical interfaces and IPv4 addresses according to your environment.
   You must add at least one static IPv4 address.

5) On the Routing pane, add a route to the Management Server through Interface 0 in one of the following ways:
   • Add a specific route to the Management Server.
     Note: The routing configuration in the SMC must be the same as the routing configuration in AWS.
   • Add a default route through Interface 0.

6) Add more routes and configure other settings according to your environment, then click Save to save and validate changes.
7) Install a license for the Forcepoint NGFW engine and bind the license to the Single Firewall element.

   Note: When you use the Bring Your own License image, you must install a license for the engine in the SMC.

8) Save the initial configuration.

   Note: Make sure that the Management Server is reachable from the engine instance.

   a) Right-click the engine and select Configuration > Save initial Configuration.

   ![Save or Upload Initial Configuration](image)

   b) Next to the Initial Security Policy field, click Select and select a policy for the engine.

   c) Select Enable SSH Daemon.

   d) Keep the Save or Upload Initial Configuration dialog box open.

Connect the NGFW Engine to the SMC

Establish contact between the NGFW Engine and the Management Server.

Steps

1) On your computer, open a terminal program, then enter the following command to connect to the command line of the NGFW Engine:

   ```
   ssh -i <your ssh private key>.pem aws@<aws instance public ip address>
   ```
2) On the command line of the NGFW Engine, enter the following command to start the NGFW Initial Configuration Wizard:

```
sudo sg-reconfigure
```

3) Configure the general settings and network interfaces for the NGFW Engine. For detailed instructions, see the *Forcepoint Next Generation Firewall Installation Guide*.

4) On the Prepare for Management Contact page, select DHCPv4 or DHCPv6.

5) Select Contact, then press the spacebar.

6) Enter the Management Server contact IP address and the one-time password.

7) Highlight Finish, then press Enter. The engine now tries to make initial contact with the Management Server. The progress is displayed on the command line. If you see a connection refused message, make sure that the one-time password is correct and the Management Server IP address is reachable from the node. Save a new initial configuration if you are unsure about the password.

   **Note:** If the initial management contact fails for any reason, you can start the configuration again with the `sg-reconfigure` command.

**Result**

After you see notification that Management Server contact has succeeded, the engine installation is complete and the engine is ready to receive a policy. The engine element’s status changes in the Management Client from Unknown to No Policy Installed. The connection state is Connected, indicating that the Management Server can connect to the node.

**Next steps**

Install a policy on the engine using the Management Client

---

**Deploy Forcepoint NGFW in AWS when you have an existing SMC installation**

If you already have an existing SMC installation, you can deploy additional NGFW Engines in AWS.

**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 documentation:

- *Forcepoint Next Generation Firewall Installation Guide*.
How to deploy Forcepoint NGFW in the Amazon Web Services cloud

- *Forcepoint Next Generation Firewall Product Guide.*

**Steps**

1) Make sure that your Management Server is reachable from your Forcepoint NGFW AWS instance.

2) In the Management Client, create a Location element for elements that are located in networks outside of the local network for the SMC servers.
   In the example configuration, a Location element called "internet" has been created.

3) Configure contact addresses for the Management Server.
   In the example configuration, the external IP address that is used to reach the SMC from AWS has been configured as the contact address for the "internet" Location.

   a) In the Management Server Properties dialog box, click Exceptions.

   b) Click Add, select the Location element that you created, then click Select.
How to deploy Forcepoint NGFW in the Amazon Web Services cloud

How to deploy Forcepoint NGFW in the Amazon Web Services cloud

In the Contact Address cell, enter the external IP address that is used to reach the SMC from AWS, then click OK.

c) Click OK to close the Management Server Properties dialog box.

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, then select the Location element that you created and click Select.

c) In the Contact Address cell, enter the external IP address of the Log Server, then click OK.

d) Click OK to close the Log Server Properties dialog box.

Create Single Firewall elements

Create a Single Firewall element for each Forcepoint NGFW engine that you deploy in the AWS cloud. These steps provide an overview of the NGFW configuration process. For detailed instructions, see the following documentation:

• Forcepoint Next Generation Firewall Installation Guide.
• Forcepoint Next Generation Firewall Product Guide.

Steps

1) Add a Single Firewall element.

2) From the Location drop-down list on the General pane, select the Location element for elements outside of the local network of the SMC servers.

In the example configuration, the "internet" Location element is used.

3) Add a layer 3 physical interface and configure it as the primary control interface.

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 DCHP Interface.

e) In the Interface Options, 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 engine opens a connection to the Management Server and maintains connectivity.

4) Add more physical interfaces and IPv4 addresses according to your environment.

You must add at least one static IPv4 address.
5) On the Routing pane, add a route to the Management Server through Interface 0 in one of the following ways:
   - Add a specific route to the Management Server.
     
     **Note:** The routing configuration in the SMC must be the same as the routing configuration in AWS.
   - Add a default route through Interface 0.

6) Add more routes and configure other settings according to your environment, then click **Save** to save and validate changes.

7) Install a license for the Forcepoint NGFW engine and bind the license to the Single Firewall element.

   **Note:** When you use the Bring Your own License image, you must install a license for the engine in the SMC.

8) Save the initial configuration.

   **Note:** Make sure that the Management Server is reachable from the engine instance.

   a) Right-click the engine and select **Configuration > Save initial Configuration.**

   ![Image of Save or Upload Initial Configuration dialog box]

   b) Next to the Initial Security Policy field, click **Select** and select a policy for the engine.

   c) Select Enable SSH Daemon.

   d) Keep the Save or Upload Initial Configuration dialog box open.
How to deploy Forcepoint NGFW in the Amazon Web Services cloud

Configure the AWS environment

Prepare the AWS environment for the NGFW deployment.

These instructions use the AWS web management console. For automated and large scale deployment, we recommend using the AWS command line interface (CLI) tools or lower level programming libraries to communicate with the AWS REST API directly.

These steps provide an overview of the configuration process. For detailed instructions, see the Amazon Elastic Compute Cloud Documentation and the Amazon Virtual Private Cloud Documentation.

Steps

1) Create the virtual private clouds (VPCs) and subnets that the NGFW engine will be connected to.

2) Create one elastic network interface (ENI) each for physical interface that you added to the Firewall element.

   Note: Do not allow AWS to automatically allocate interfaces.

3) Disable the Source/Dest. check option for each engine interface.

   The Source/Dest. check option prevents packet forwarding to destinations on other interfaces. When the option is enabled, the firewall cannot act as a router.

   a) Right-click the ENI interface and select Change Source/Dest. Check.

   b) From the Source/Dest. check options, select Disabled.

   c) Click Save.

4) Create subnets and assign them to interfaces.
5) Create the required gateways and routing tables and assign them to subnets.

Create a Forcepoint NGFW instance using Manual Launch

Configure and launch an instance of the Forcepoint NGFW AMI using Manual Launch.

**Before you begin**

Before you begin, make sure that the Management Server is reachable from the instance.

⚠️ **CAUTION:** To protect the privacy of your data, we recommend using dedicated instances when you deploy Forcepoint NGFW in AWS.

**Steps**

1) In the AWS Marketplace, start the launch for the Forcepoint NGFW AMI.

2) Click the Manual Launch tab.

3) Select an instance type that meets your performance needs.

   The AMI automatically restricts the instance types so that only compatible instance types are available.

4) Add one or more interfaces and map ENIs to the interfaces.

   a) To add an interface, click Add Device.

   ⚠️ **Note:** The wizard only allows you to add two interfaces. If you need to add more interfaces, use the command line tools.

      Add all required interfaces while creating the instance. If you add interfaces later, a reboot is required before the interfaces become available.

   b) From the Network Interface drop-down list for eth0, select the ENI for the control interface.

   c) From the Network Interface drop-down list for the other interfaces, select the ENI to connect to each interface.
5) If you want to transfer the initial configuration file to the instance, add the initial configuration as user data.

**Note:** We recommend transferring the engine's initial configuration as user data when you launch the Forcepoint NGFW instance. When you provide user data, the engine automatically makes initial contact with the Management Server when it starts. After it is launched, the Forcepoint NGFW instance automatically appears in the Management Client. If you launch the instance without user data, you can manually make initial contact with the Management Server using the sg-reconfigure script on the engine's command line.

![Advanced Details](image)

a) In the User Data options, select As Text.

b) In the Save or Upload Initial Configuration dialog box in the Management Client, click Copy to Clipboard.

c) In the EC2 Management Console, paste the text into the User Data field.

6) Click Review and Launch.

7) On the Review Instance Launch page, select an existing key pair or create a new key pair for SSH connections to the NGFW engine.

**Note:** The key is the only allowed authentication method for SSH connections to the engine command line.

If the default security group is too limited for your environment, you can use a different security group or change the rules. You can also configure the NGFW Engine to restrict access.

### Troubleshooting

You can use diagnostics information provided by the AWS console for troubleshooting.

If the SSH service for the engine does not start automatically, use the Actions > Instance Settings > Get system log option to get diagnostics information.
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.